NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE RISKY SHIFT TOWARD ONLINE ACTIVISM: DO HACKTIVISTS POSE AN INCREASED THREAT TO THE HOMELAND?

by

Brian C. Murphy

September 2014

Thesis Co-Advisors: Nadav Morag
John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
THE RISKY SHIFT TOWARD ONLINE ACTIVISM: DO HACKTIVISTS POSE AN INCREASED THREAT TO THE HOMELAND?

5. FUNDING NUMBERS

6. AUTHOR(S) Brian C. Murphy

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This research uses a grounded theory approach to study the phenomenon of hacktivism and seeks to understand how the Internet has evolved to become a disproportionate and significant platform for disruption. Technological advancements involving the Internet, such as social media, have provided a significant advantage for social activists to advance their causes and enables them to recruit large masses with little effort. This platform also provides the distinct advantage of anonymity and increased availability of malicious tools and malware that, if directed toward U.S. critical infrastructure, could potentially cause severe economic and physical harm to the homeland. This research will also provide readers an in-depth analysis of three well-known social movements that have revealed the potential for increasing violence and/or disruption. The civil rights movements of the 1960s and the environmentalist movements of the 1980s are examples of activist movements that quickly evolved into direct action networks. Such historical context, when compared to current hacktivist collectives like Anonymous, suggests that social activist movements, regardless of venue, possess the cognitive praxis to cause injury or harm in furtherance of a social cause.

14. SUBJECT TERMS hacktivism, activism, Anonymous, social movement, Internet, hackers; cyber; anonymity, Earth First!, Students for a Democratic Society (SDS), hacktivist, social media, social activist

15. NUMBER OF PAGES
157

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE RISKY SHIFT TOWARD ONLINE ACTIVISM: DO HACKTIVISTS POSE AN INCREASED THREAT TO THE HOMELAND?

Brian C. Murphy
Special Agent in Charge, United States Secret Service
B.S., Fordham University, 1991

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND DEFENSE AND SECURITY)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2014**

Author: Brian C. Murphy

Approved by: Nadav Morag
Thesis Co-Advisor

John Rollins
Thesis Co-Advisor

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research uses a grounded theory approach to study the phenomenon of hacktivism and seeks to understand how the Internet has evolved to become a disproportionate and significant platform for disruption. Technological advancements involving the Internet, such as social media, have provided a significant advantage for social activists to advance their causes and enables them to recruit large masses with little effort. This platform also provides the distinct advantage of anonymity and increased availability of malicious tools and malware that, if directed toward U.S. critical infrastructure, could potentially cause severe economic and physical harm to the homeland. This research will also provide readers an in-depth analysis of three well-known social movements that have revealed the potential for increasing violence and/or disruption. The civil rights movements of the 1960s and the environmentalist movements of the 1980s are examples of activist movements that quickly evolved into direct action networks. Such historical context, when compared to current hacktivist collectives like Anonymous, suggests that social activist movements, regardless of venue, possess the cognitive praxis to cause injury or harm in furtherance of a social cause.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ALF	Animal Liberation Front
APT	advanced persistent threat
BHP	BayerischerHackPost
CIP	critical infrastructure protection
CoS	Church of Scientology
DARPA	Defense Advanced Research Projects Agency
DDoS	distributed denial of service
DHS	Department of Homeland Security
ELF	Earth Liberation Front
FBI	Federal Bureau of Investigation
GAO	General Accountability Office
HBG	HBGary Federal
IP	Internet Protocol
IT	information technology
LOIC	low orbit ion cannon
LulzSec	Lulz Security
NASA	National Aeronautics and Space Administration
NSA	National Security Agency
PGP	Pretty Good Privacy
PL	Progressive Labor Party
RYM	Revolutionary Youth Movement
SDS	Students for a Democratic Society
SIT	social identity theory
TCP	Transmission Controls Protocol
Tor	The Onion Router
WUO	Weather Underground Organization

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

There has been a limited amount of research conducted on the potential for hacktivism and collectives like Anonymous to continue to evolve into a potent homeland security threat. Hacktivism has become increasingly prominent over the last few years and has been largely ignored as a potential threat to the critical infrastructure in the United States despite its own repeated warnings. This thesis focuses on the potential for hacktivism to emerge into more disruptive movements and whether such web based collectives are distinctly advantaged over previous social movements. As America's critical infrastructure becomes increasingly entwined with the global web, it is important to understand whether hacktivist movements possess the praxis to become an increasingly disruptive global force and threat to America's homeland.

Currently, homeland security officials target hacktivists after they have already engaged in disruptive behavior often times at great expense to America's corporate and government sectors. However, this strategy fails to recognize the fact that unlike previous terrestrial social movements, web-based hacktivist groups are distinctly advantaged at formulating collective action on a global scale. Evolving out of an online collective, hacktivists take advantage of weaponized malware and tools to cause disruptive acts, often times leading to tens of millions of dollars in loss to private and corporate sector companies in America. As a global collective, targeting one or more hacktivists does not eliminate the threat since the Internet provides access to an infinite and resilient resource capable of extending the life cycle of the hacktivist's action and threat.

This research uses a grounded theory approach to study the phenomenon of hacktivism and seeks to understand how the Internet has evolved to become a disproportionate and significant platform for disruption. Technological advancements involving the Internet, such as social media, have provided a significant advantage for social activists to advance their cause enabling them to recruit large masses with little effort. This platform also provides the distinct advantage of anonymity and increased availability of malicious tools and malware that, if directed towards U.S. critical infrastructure, could potentially cause severe economic and physical harm to the

homeland. This research will also provide readers an in depth analysis of three well-known social movements that have revealed the potential for increasing violence and/or disruption. The civil rights movements of the 1960s and the environmentalist movements of the 1980s are two examples of activist movements that quickly evolved into direct action networks. Such historical context when compared to current hacktivist collectives suggests that social activist movements, regardless of venue, possess the cognitive praxis to cause injury or harm in furtherance of a social cause.

This thesis is not intended to argue or necessitate action against online activism but rather increase awareness for an underappreciated threat that is likely to continue to evolve into a more disruptive force. In 2011, the "re-imagined and re-invigorated specter of '"hacktivism"' rose to haunt organizations around the world" supplanting the cyber criminal and state sponsored hacker as the most prevalent threat on the Internet.[1] The actual threat posed by the hacktivist is subject to much debate; however, increased hacktivist activities suggest that the security environment in cyberspace is changing.

The rise of hacktivism is no accident. Technological advancements involving the Internet, such as social media, have provided a significant advantage for activists to advance their cause, which enables them to recruit large masses with little effort. This platform also provides the distinct advantage of anonymity, a luxury not previously enjoyed by leaders of traditional social movements. More concerning; however, is the increasing availability of malicious tools and malware that, if directed towards U.S. critical infrastructure, could potentially cause severe economic and physical harm to the homeland. However, what makes hacktivism unique and different from criminal organizations is also what makes it more challenging. The lack of structure to the hacktivist movement is the basis for its strength and potential for increasing its dangerousness. Hacktivism, unlike the organized criminal group and nation state, is a leaderless phenomenon that has little accountability. This amorphous nature limits our

[1] Verizon, *2012 Data Breach Investigations Report*, Verizon Enterprise, 2012, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

ability to predict the trajectory of hacktivist actions since leaderless movements lack direction and discipline.[2]

Hacktivist actions are learned in the social environment and through social interaction. As activist societies exist in complex social environments and adapt themselves to these environments, the hacktivist adapts within the virtual cyber environment. Recent data breach reports suggest hacktivist groups are evolving from peaceful online protest action towards more aggressive and disruptive acts.[3]

In 2013, the hacktivist group Anonymous secretly accessed U.S. government computers and stole sensitive information in a yearlong campaign with yet to be determined consequences.[4] The easy availability of cyber based weapons have been used by hacktivists to cause millions of dollars in damage to government and private and commercial sector companies and organizations that are currently disadvantaged in defending against the nature of the hacktivists threat. Purposeful use of these weapons has already caused significant harm to critical infrastructure in nations like Iran, Estonia and the U.S.; however, hacktivists have yet to join the fray.

Much like terrestrial based social movements, hacktivist groups like Anonymous are challenged by its diversity of membership and the number of competing issues that dilute its debate. Online collectives purposely use discourse and debate to increase issue awareness and identify those issues with a need for action. However, much like terrestrial based social movements, harmful acts defeat their purpose offering requiring restraint to maintain the support of its majority. This mainstream effort isolates more extreme members within the movement who, now unaligned with the majority, are forced to splinter form the group to carry out more violent, or in the case of hacktivism, more disruptive action.

---

2 Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013).

3 Francios Paget, *Cybercrime and Hacktivism*, McAfee Labs, http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf.

4 "FBI Warns That Anonymous Has Hacked US Government Sites for a Year," *The Guardian*, November 16, 2013, http://www.theguardian.com/technology/2013/nov/16/anonymous-fbi.

Projecting the course of hacktivism is difficult; however, this thesis has shown that social movements, regardless of venue, have the praxis to evolve and splinter into more radical groups. Purposeful actions are carried out by minority members who formulate their own clusters based upon ideology and competence. For hacktivists, the Internet accelerates the process of collective identity. The threat is realized from resulting small clusters that splinter from the majority in order to sustain a secure operating environment and endorse more forceful action. Resulting law enforcement actions against these groups do not necessarily reflect failure of the movement since, as noted by Christina Foust assistant professor of communication studies at the University of Denver, such repressive effects "are felt as a reclamation of agency and autonomy in the present, as well as the future."[5] Thus, the transgressive clusters within Anonymous and other activist movements have ability to inspire future action. The provocative comments of members of Anonymous subsequent to the arrests of many of its members suggest a natural evolution of the web-based social movement. Anonymous and other Internet based movements have a never-ending pool of resource. To successfully control them will require even greater resource suggesting, "hacktivism cannot be stopped any more than activism can."[6] The vulnerability of the Internet, availability of cyber based weapons, and threat of imminent action signals a hacktivist threat that is very real.

[5] Christina R. Foust, *Transgression as a Mode of Resistance: Rethinking Social Movement in an Era of Corporate Globalization* (London: Lexington Books, 2010).

[6] Michael Colesky, and Johan Van Niekerk, *Hacktivism: Controlling The Effects* (Port Elizabeth, South Africa: Nelson Mandela Metropolitan University), http://www.academia.edu/2033252/Hacktivism_-_Controlling_The_Effects.

ACKNOWLEDGMENTS

I want to express my deep thanks to my esteemed advisors Nadav Morag and John Rollins for their insightful discussion, valuable advice, and support during the writing process. Your patience and guidance during this period was truly appreciated.

Many friends and cohorts have helped me stay sane throughout this difficult process. I greatly value their friendship, and I deeply appreciate their sense of humor throughout the whole process. Cheers!

Most importantly, I would like to thank my wife, Deirdre, and my children Kiera, Caitlin, and Jillian, whose patience and support made completing this program a reality. I could not have completed this work without their encouragement and understanding, and most importantly, their unconditional love. Thank you and love always!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE PROBLEM

This thesis explores whether social and technological advancement involving the Internet have increased the threat posed by hacktivists to our homeland and whether such web-based activist movements can evolve into more serious disruptive actors. Today's technological advancements would enable a cyber activist, if so willing, to utilize increasingly sophisticated cyber tools to further the activist cause. This research will attempt to provide a better understanding of the Internet as a platform for disruption and whether web-based social movements have the praxis to evolve and/or splinter into increasingly more disruptive forces for change.

Globalization would be difficult to imagine without the creation of the Internet.[7] The Internet provides methods of communication that enable people from opposite ends of the globe to openly exchange information and share ideas. However, while the Internet has proved to be "largely resilient to attacks and other disruptions so far," the increased connectivity and reliance on the web suggests a changing environment for disruption.[8] Today, a threat through the Internet means a threat to everything.[9] Yet, despite this increased risk, web-based social movements continue to evolve online with increasing sophistication and resiliency. Groups like Anonymous have caused hundreds of millions of dollars in damage and lost revenue to government and private sector entities with little or no remedy. Defending against such threats is difficult at best and will likely remain that way with increased availability and sophistication of web-based weapons and tools. As threat actors on the web, it is worthwhile to study hacktivist movements and the level of risk posed by such groups. What role does the Internet play in the creation of these groups and the decision to formulate action? Are web-based social movements

---

[7] National Council on Economic Education, *Thinking Globally: Effective Lessons for Teaching about the Interdependent World Economy: Lesson 1: Ten Basic Questions about Globalisation* (New York: National Council on Economic Education, 2005), http://www.imf.org/external/np/exr/center/students/hs/think/lesson1.pdf.

[8] World Economic Forum, *Global Risks 2014*, 9th ed. (Geneva, Switzerland: World Economic Forum, 2014), http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, 38.

[9] Ibid., 39.

significantly advantaged over terrestrial-based movements such that their very existence implies an increased security risk to the homeland?

There is a limited body of literature that discusses hacktivism in the context of social movements and how web-based movements may evolve. By studying the evolution of social movements, this thesis will attempt to identify possible trigger points or casual factors for increased risk of violence in social movements. These findings, when applied to hacktivism, will possibly reveal whether the praxis exists for cyber activists to increase their disruptive actions concurrent with the increasing sophistication of Internet based tools and software capabilities. In further describing the nature of the Internet based threat, research will be conducted to identify potential factors that distinguish hacktivism as an increased risk from other activist movements.

B. BACKGROUND

In 2011, the "re-imagined and re-invigorated specter of 'hacktivism' rose to haunt organizations around the world" supplanting the cyber criminal and state sponsored hacker as the most prevalent threat on the Internet.[10] The actual threat posed by the hacktivist is subject to much debate; however, increased hacktivist activities suggest that the security environment in cyberspace is changing. The phrase hacktivism was first coined by the hacker collective Cult of the Dead Cow and was intended to refer to the use of technology to foster human rights and the open exchange of information.[11] The term has since evolved to characterize cyber-based activist efforts that may include protest "sit in" equivalents, such as denial of service attacks or website defacements, to more destructive hacking attacks against government or private computer networks.

1. Cyber Threat

Different threat actors with different intentions and capabilities challenge the cyber security environment on many fronts. Nation states and organized criminal groups represent the most sophisticated, persistent, and resourced of any advanced actors on the

[10] Verizon, *2012 Data Breach Investigations Report*, 2.

[11] Michelle Delio, "Hacktivism and How It Got Here," *Wired*, July 14, 2004, http://www.wired.com/techbiz/it/news/2004/07/64193?currentPage=all

Internet capable of waging sustained efforts using a variety of sophisticated tools to achieve their goals.[12] Despite demonstrating the capability and intent to persistently and effectively target the government and private sectors, hacktivists are perceived by some to be a limited threat whose actions are rather simple expressions of civil disobedience. Hacktivists linked to the collective group Anonymous went so far as to petition the U.S. government to decriminalize their denial of service attack methods and make them a legal form of protesting.[13]

Illicit cyber activity is not unique to hacktivist actions and is also attributed to organized crime and nation states. Nation states engage in sophisticated Internet espionage efforts against foreign government and private sector entities. Similarly skilled techniques are used by a newer breed of organized criminals who use the Internet for illicit gains by targeting an ever-expanding victim set of individuals and private sector entities who rely on the Internet for business and commerce. Despite best efforts, many of these private sector entities are finding it increasingly difficult to defend against the sustained and skilled efforts of these online threat actors, otherwise known as an advanced persistent threat (APT).[14] Since they are designed to break into networks and harvest valuable pieces of information over extended periods of time, APT attacks are purposeful and not random. APT attackers are either motivated by corporate espionage designed to steal valuable trade secrets and intellectual property, or to sabotage an organization's plans and infrastructure. According to Symantec, the attackers leverage information from a variety of sources to carefully engineer their way into a system or network.[15] This can be achieved through a number of tactics; however, the most common of which are social engineering tactics like spear phishing (an act of sending fraudulent

---

[12] White House, *Strategy to Combat Transnational Organized Crime* (Washington, DC: Executive Office of the President, 2011), http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

[13] *The Current State of Cybercrime 2013: An Inside Look at the Changing Threat Landscape*, EMC Corporation, 2013, http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf.

[14] *Advanced Persistent Threats (APTs)* (Atlanta, GA: Damballa, 2010), https://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf.

[15] Symantec, *Advanced Persistent Threats: A Symantec Perspective*, Symantec Corporation, http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

emails for the purpose of gaining unauthorized access into a system). Once inside, the attacker, intent on remaining undetected, uses sophisticated malware and anonymization tools to mask his or her actions and successfully exfiltrate or catalog data for future exploit.

The rise of hacktivism is no accident. Technological advancements involving the Internet, such as social media, have provided a significant advantage for social activists to advance their cause and enables them to recruit large masses with little effort. This platform also provides the distinct advantage of anonymity, a luxury not previously enjoyed by leaders of traditional social movements. More concerning, however, is the increasing availability of malicious tools and malware that, if directed towards U.S. critical infrastructure, could potentially cause severe economic and physical harm to the homeland.

2. Hacktivism

Depending upon one's lens, the term hacktivism can be defined from ethical acts of hacking to effect social change to outright cyber terrorism intent on massive disruption. Despite these differences, hacktivism can largely be termed an act of protest using the web-based tools to effect social or policy change or an elevation of civil disobedience into cyber space. The hacktivist, taking advantage of the cyber platform and web-based cyber weapons, formulates direct action potentially on a global scale. However, what makes hacktivism unique and different from APT and other cyber-based threats is also what makes it more challenging. Hacktivism, unlike the organized criminal group and nation state, is a leaderless phenomenon that has little accountability. This amorphous nature limits our ability to predict the trajectory of their actions since leaderless movements lack direction and discipline.[16] The 2012 Verizon *Data Breach Investigations Report* as well as actions by hacktivist groups are suggestive of a possible evolution from peaceful online protests to aggression.[17] In 2013, Anonymous secretly accessed U.S. government computers and stole sensitive information in a yearlong

[16] Rid, *Cyber War Will Not Take Place*.

[17] Verizon, *2012 Data Breach Investigations Report*.

campaign with yet to be determined consequences.[18] The Russian nationalist group Nashi demonstrated the power of cyber attack as a political tool when the group crippled Estonia's commerce through a series of Internet based denial of service attacks against Estonia's banking and government infrastructure in 2007.[19] Security experts, including the Director of the National Security Agency (NSA), General Keith Alexander, are increasingly concerned about the emerging ability within the next year or two for hacktivist groups like Anonymous to bring about power outages and disable compute networks.[20]

3. Splintering into Extremist Movements

Due to the growing dependence and interconnectivity on the Internet, it is worth asking whether the growth of hacktivism equates to a growing threat or is quite possibly a benign "computer enabled assault on violence itself."[21] Thomas Rid, author of *Cyber War Will Not Take Place*, offers an opposing discussion that suggests social movements on the web are a preferable alternative to terrestrial-based movements since the web does not possess physical characteristics of violence. Historically, traditional social movements have revealed the potential for increasing violence. The civil rights movements and anti-Vietnam War protests of the 1960s are such examples of activist movements that quickly evolved into direct action networks, such as the Weathermen.[22] The moderate protest tactics of the environmental movement were continuously suppressed by authority, which led to more extreme members to leave Earth First! to form a more violent group. Such historical context suggests that social activist

---

[18] "FBI Warns That Anonymous Has Hacked US Government Sites for a Year," *The Guardian*.

[19] Noah Schachtman, "Kremlin Kids: We Launched the Estonian Cyber War," *Wired*, March 11, 2009, http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/; Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardians*, May 16, 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia.

[20] Siobhan Gorman, "U.S. Official Warns About 'Anonymous' Power Play," *Wall Street Journal*, February 21, 2012, http://online.wsj.com/news/articles /SB10001424052970204059804577229390105521090.

[21] Rid, *Cyber War Will Not Take Place*, xiv.

[22] Ron Jacobs, *The Way the Wind Blew: A History of the Weather Underground* (London, United Kingdom: Verso Books, 1997).

movements, regardless of venue, possess the cognitive praxis to cause injury or harm in furtherance of a social cause.

Hacktivist actions are learned in the social environment and through social interaction. As activist societies exist in complex social environments and adapt themselves to these environments, the hacktivist adapts within the virtual cyber environment. According to a recent report from EMC Corporation (EMC), hacktivists are finding business opportunities and supplemental revenue streams in the underground by selling their stolen information to profit driven criminals.[23] With weaponized malware variants increasingly available to cybercriminals, does this new crossover collaboration push hacktivist actions further along the threat continuum?[24]

America's networks will continue to be challenged by new forms of hacking concurrent with challenges to the nation's political structure. Academic analysis of the evolution of hacktivism is necessary to better understand the current and potential future threat to such systems posed by the increasingly skilled hacktivist. The cyber radical has many faces. Should the growth of this social movement lead us to caution and fear or, according to some, hope and exhilaration?[25]

C. LITERATURE REVIEW

This review identifies relevant sources concerning hacktivism and the differing social opinions regarding the threat or lack of threat posed by hackers who use the Internet to effect social or political change. Since hacktivism is generally agreed to have emerged in the late 1980s, the scope of the literature review reaches back to its emergence in the late 1980, when hacktivism is generally agreed to have started. Within this review, numerous sources have been identified to support analysis and understanding of social movements, hacktivist actions, identity issues concerning hacktivist groups, and the threat or lack thereof posed by hacktivists.

---

[23] *The Current State of Cybercrime 2013: An Inside Look at the Changing Threat Landscape*.

[24] *Weaponized Malware: A Clear and Present Danger* (WP-EN-09-12-12), Lumension, September 2012, https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Whitepapers/Weaponized-Malware---A-Clear-and-Present-Danger.aspx.

[25] Kat Braybrooke, "Hacktivism Is Unbound," Tumblr.com, http://hacktivism-is-unbound.tumblr.com/.

Much has been written regarding hacktivism that recounts the first reported hacktivist protest in 1989 involving the release of the "WANK worm" into the National Aeronautics and Space Administration's computer network. This anti-nuclear protest called attention to the launch of a plutonium powered satellite and is one of many actions that continue to grow in sophistication and impact.[26] According to NSA Director General Keith Alexander, hacktivist collectives such as Anonymous pose an increasing risk to our national security.[27] Anonymous members immediately denied such accusations despite having threatened to take down the Internet only one week earlier.

The literature review of hacktivism is broad and, for the purposes of this initial research, is separated into four categories. The first addresses the ethos of the hacktivist movement and whether such actions are in fact an ethical form of civil disobedience in a new social construct of reality. There is differing opinion on the value of the hacktivist action in regards to free speech. The second and third sections will address the discussion concerning hacktivist actions and tactics and whether these actions are effective in creating social or political change. The final section will address the discourse about whether hacktivism represents an emerging threat to the homeland. The research suggests divergent opinions on each of these issues.

Since the first hacktivist action in 1989, the size of the Internet has exploded and with it the number and increasingly sophisticated forms of online protests and political activism. Forms of protest have varied to defacement of websites, to hacking of financial infrastructure to outright cyber warfare against countries like Georgia and Estonia. Yet, despite these actions, the research differs on whether hacktivist groups such as Anonymous truly are a threat or, as one researcher believes "not inherently dangerous" but rather "important tools for realizing social change."[28]

---

[26] Suelette Dreyfuss, *Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier* (Sydney, Australia: Random House Australia 1997).

[27] Gorman, "U.S. Official Warns About 'Anonymous' Power Play."

[28] Victoria McLaughlin, *Anonymous: What Do We Have to Fear from Hacktivism, the Lulz, and the Hive Mind?* (Charlottesville, VA: University of Virginia, 2012), https://pages.shanti.virginia.edu /Victoria_McLaughlin/files/2012/04/McLaughlin_PST_Thesis_2012.pdf, 81.

1. A New Social Reality?

Hacktivism is a scaled form of political activism that includes modern forms of civil disobedience to more radical attacks against critical infrastructure. Eric Sterner further described the cyber protest movement as "American as apple pie" and stated that the ends fit well within American tradition.[29] Such situations or events are perhaps conceptualized as "changing strategies of argumentation" utilizing new social tools and are, as theorized by Corbett in his individual research on reasoning, as antiquated as Plato and Aristotle.[30] Social discourse has historically been accepted throughout the ages; yet, there are many examples of when such discourse pushed the boundaries of disagreement during the course of social argument and press upon the fringe of immediate recourse for change. The Earth Liberation Front (ELF), a radical environmental group, was formed by a group of frustrated British Earth First! members who were dissatisfied by the organization's desire to abandon illegal tactics.[31] In his analysis of ELF, Loadenthal surmised that Earth First!'s ideological underpinnings are based in "deep ecology, anti-authoritarian anarchism highlighting a critique of capitalism, a commitment of non-violence, a collective defense of the Earth."[32] The group has since evolved into the Earth Liberation Front and is more closely recognized as a collective of autonomous individuals who utilize illegal tactics, such as sabotage and vandalism, in furtherance of their ideological beliefs. The Federal Bureau of Investigation has classified ELF as a domestic terrorist group in 2001. Yet, despite this regulatory action, social movements as a form of resistance have continued to progress in many ways. David Heineman, in his thesis about digital rhetoric, succinctly equates hacktivist actions as forms of visual or

---

[29] Eric Sterner, *The Paradox of Cyber Protest* (Arlington, VA: George C. Marshall Institute, 2012), http://marshall.org/wp-content/uploads/2013/12/Paradox-PO-Apr-12.pdf, 1.

[30] P. J. Edward Corbett, "The Changing Strategies of Argumentation from Ancient to Modern Times," in *Practical Reasoning in Human Affairs: Studies in Honour of Chaim Perelman*, ed. James L. Golden and Joseph J. Pilotta, 21–36. 1st ed. (Dordrecht, Netherlands: Springer, 1986).

[31] Paul Joosse, "Leaderless Resistance and Ideological Inclusion: The Case of the Earth Liberation Front," *Terrorism and Political Violence* 19 (2007): 351–68.

[32] Michael Loadenthal, "The Earth Liberation Front: A Movement Analysis," *Radical Criminology*, no. 2 (2013): 15.

ocular arguments evidenced by website defacements and message board discussions.[33] The terrestrial movement made cyber.

If argumentation theory is valid, then to what end is the level of online discourse considered an acceptable reality? It is hard to argue that in the new age of social media, today's generation is becoming increasingly adept at utilizing the Internet as a primary form of communication. In this context, personal communication as a form of face-to-face interaction is clashing with the increasingly growing culture of online communication. In this backdrop, the hacktivist movement has gained strength and increased notoriety.

As previously noted, General Alexander highlighted the U.S. government's concern that Anonymous potentially represents an increased threat to our homeland security threat. In their widely accepted publication the *Social Construction of Reality*, Berger and Luckmann demonstrate that persons and groups through a period of interaction within a social system will begin to adopt or habitualize each other's actions eventually institutionalizing these actions as the new norm.[34] If accepted, then it can be said hacktivism is an expression of the new argumentation reality online. Sociologist Herbert Blumer views collective behavior as key towards breaking normal, institutionalized behavior thus positively contributing to society.[35] The websites Reddit.com and Change.org are widely accepted social activist platforms for ideological discussion; however, why then do the hacktivist actions of Anonymous not receive similar acclaim or acceptance? If reality is socially constructed, then over time is it likely that hacktivist actions will also become more widely accepted or will they evolve into more similar movements such as ELF?

The recent comments attributed to Director of the NSA, General Keith Alexander appear to suggest that the U.S. government does not share Blumer's principle when it

---

[33] David Scott Heineman, "The Digital Rhetorics of Hacktivism: Anti-Institutional Politics in Cyberspace" (master's thesis, University of Iowa, 2007).

[34] Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (Garden City, NY: Anchor Books, 1967).

[35] Ron Eyerman and Andrew Jamison, *Social Movements: A Cognitive Approach* (University Park, PA: The Pennsylvania State University Press, 1991).

comes to the newly evolving phenomenon of hacktivism. General Alexander believes that the threat posed by protest groups of hacktivists are sources for considerable concern and suggests that in the very near future, such groups will have the ability to attack the electrical grid.[36] The increased threat posed by Anonymous and the hacktivist collective is potentially supported by the increasing number of sophisticated attacks against U.S. government and corporate targets.[37] As a newly evolving phenomenon, it is worthwhile to examine the identity of Anonymous and whether its acceptance or lack thereof is attributable to generational clash or nonconforming realties.

2. The Hacktivist in Action

Perhaps the most pertinent discussion concerning reality is that offered by Jean Baudrillard in his essay entitled "The Violence of the Image." Baudrillard asserts that the act of becoming, that is, the environmentalist achieving all things green or the hacktivist realizing a world void of censorship, is an "image produced in real time" theoretically ending the period of becoming or action to achieve this goal.[38] However, actuality "does not know anything but change, it does not know the concept of becoming." Many groups have evolved or changed purpose for both good and nefarious cause. The March of Dimes, created to find a cure for polio, has since evolved its mission to increase awareness of a variety of health issues facing mothers and babies. Thus, according to Baudrillard, the change of purpose means the image can never be realized. What then of the hacktivist movement in the current context of the Internet? To what end will Anonymous go to achieve an ever-distant goal?

In the processing of becoming, Samuel, in her thesis concerning hacktivism and the future of political participation, suggests that hacktivists, perhaps emboldened by the Internet's perceived anonymity, is increasingly focused on the "right to be heard—rather

---

[36] Gorman, "U.S. Official Warns About 'Anonymous' Power Play."

[37] Verizon, *2013 Data Breach Investigations Report*, Verizon Enterprise, 2013, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

[38] Jean Baudrillard, "The Violence of the Image," European Graduate School, accessed January 7, 2014, http://www.egs.edu/faculty/jean-baudrillard/articles/the-violence-of-the-image/.

than the simpler right to speech itself" and is capable of more direct action.[39] Under the guise of hacktivism, groups such as Anonymous appear to achieve legitimacy; however, it is under this guise that the potential may emerge for more sinister action. In 2011, Anonymous and its splinter group LulzSec engaged in an aggressive cyber campaign against numerous private and government sector entities. Sophisticated denial of service attacks and network hacks resulted in disruption of commerce and banking as well as the release of sensitive email information and credit card account numbers.[40]

The narrative concerning the legitimacy of hacktivism is broad and ranges from message board banter towards, according to Sterner, cyber warfare like that experienced by the country of Georgia in 2008. Sterner suggests that the hacktivist movement creates a sense of insecurity that no longer draws attention to a cause but rather to the movement itself.[41] The shift away from simply organizing or expressing opinions about an institution to outright cyber attacks is a potential reflection of the changing landscape in the hacktivist movement.

3. An Identity Problem

The Anonymous collective as a social movement, although powerful in the cyber arena, is not unlike other terrestrial social movements. Denning roughly describes the hacktivist movement as a leaderless resistance that typically operates without the constraints of command and control or official rules and procedures.[42] Similar groups, such as ELF and the modern anarchist movement, have operated under these same environs with limited result yet continue to endure.

---

[39] Alexandra Samuel, "Hacktivism and the Future of Political Participation" (master's thesis, Harvard University, 2004), http://www.academia.edu/616169/Hacktivism_and_the_future_of_political_participation, 234.

[40] Quinn Norton, "2011: The Year Anonymous Took on Cops, Dictators and Existential Dread," *Wired*, January 11, 2012, http://www.wired.com/threatlevel/2012/01/anonymous-dicators-existential-dread/3/

[41] Sterner, *The Paradox of Cyber Protest*.

[42] Dorothy E. Denning, "Cyber Conflict as an Emergent Social Phenomenon," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (Hershey, PA: Information Science Reference, 2011), http://faculty.nps.edu/dedennin/publications/CyberConflict-EmergentSocialPhenomenon-final.pdf.

The lack of structure to the hacktivist movement is the basis for its strength and potential for increasing dangerousness. The emergence of social media has enabled groups such as Anonymous to increase online support with some passive members willing to facilitate the distribution of automated software tools developed by the more active and skilled members of the group. According to Denning, the tools themselves give the group leaders the control over the conduct of attack.[43] The growth of online forums has contributed to the growth of the hacktivist phenomenon and must be considered when evaluating the movement as an emerging threat to homeland security. Very simply, the online forum provides means for distributing cyber attack tool(s), communicating targets to attack, and the necessary coordination for success.[44] However, the anonymity afforded by social media and other web-based tools obscures the true identity of the hacktivist movement. This problem of identity makes it difficult to pin down purpose or motivation prompting leading researcher Thomas Koenig to ask "is Anonymous more a subculture with a franchise name than a hacktivist-movement?"[45]

Schwartz, Dunkel, and Waterman, in their article entitled "Terrorism: An Identity Theory Perspective," discuss terrorism as a multifaceted problem that can be better understood when analyzed through the lens of identity theory.[46] Strindberg provides further support in suggesting that social identity theory (SIT) provides a broad analytical framework for understanding groups in general thus possibly encompassing the hacktivist collectives Anonymous and LulzSec.[47] Although hacktivist actions are not yet widely attributed as terrorism, SIT, and other identity theories may provide the necessary frameworks to evaluate hacktivist groups and similar structured movements. According to Strindberg, the SIT framework helps researchers to better understand general patterns

---

[43] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt, 239–288 (Santa Monica, CA: RAND, 2001).

[44] Ibid.

[45] Thomas Koenig, "Anonymous: Merely a Causal Consequence of Social Media?" Shabka, August 7, 2013, http://www.shabka.org/2013/08/07/anonymous-consequence-of-social-media/.

[46] Seth Schwartz, Curtis Dunkel, and Alan Waterman, *Terrorism: An Identity Theory Perspective, Studies in Conflict & Terrorism* (New York: Routledge, 2008).

[47] Anders Strindberg, "Social Identity Theory and the Study of Terrorism," unpublished, Naval Postgraduate School.

of behavior possibly alerting us to the socially conditioned traits and behaviors present in past and possibly future behaviors.[48]

Halupka states that the issue of online activism can be identified on two main levels: individual/participant and collective/community, thus complicating the role of identity in the hacktivist movement.[49] In addition, Halupka highlights the need for further identity analysis in attempting to understand the way Anonymous and similar groups will facilitate future political participation in their attempts to incite social reform.

Gabriella Coleman, author of numerous publications concerning the group Anonymous, calls for a more critical engagement of protest politics online.[50] According to Coleman, "We need to start asking more specific questions about why and when hackers embrace particular attitudes toward different kinds of laws, explore in greater detail what they are hoping to achieve, and take greater care in examining the consequences."[51]

4. Persistent Threat?

As the private and government sectors continue to increase their online presence and dependence on the Internet, they will become increasingly vulnerable to the effects of cyber protests. Gunter Ollman, Vice President of Research for Damballa, suggests that the steady increase in the sophistication of hacker tools combined with the social network and the general availability of "military grade" cyber attack tools make it a "trivial task for protestors to launch crippling attacks from anywhere around the world."[52] This is supported by the Georgia Institute of Technology in its 2013 emerging cyber threats report that suggests that malware developers are experimenting with new ways to foil

---

48 Ibid.

49 Max Halupka, "The Evolution of Anonymous as a Political Actor" (master's thesis, Flinders University of South Australia, 2011).

50 Gabriella Coleman, "Our Weirdness Is Free," accessed January 8, 2014, http://canopycanopycanopy.com/issues/15/contents/our_weirdness_is_free.

51 Ibid.

52 Gunter Ollmann, *The Opt-In Botnet Generation: Social Networks, Hacktivism and Centrally-Controlled Protesting*, Damballa, 2010, https://www.damballa.com/downloads/r_pubs/Opt-In_Botnets.pdf, 1.

defensive measures against denials of service tactics and other favorite hacktivist tactics.[53] As noted by the 2012 *Verizon Data Breach Report*, hacktivist continue to focus on the government and financial sectors.[54] What is not entirely clear is the extent to which the government and private sectors have prepared to defend against hacktivist tactics.

History is replete with examples of social movements such as the 1920s German Nazi Party and the civil rights and anti-Vietnam War movements of the 1960s that have fractured into more disruptive movements.[55] Although literature concerning social movement theory provides context for these movements, little is offered as to why these movements fracture to form more disruptive, sometimes terroristic, groups. The environmental movement of the 1970s spawned more active groups, such as Greenpeace and Earth First!, each dissatisfied with perceived ineffectiveness of political advocacy and legislation concerning the environment.[56] The manifestation of the environmental movement varied from country to country; however, the movement was and remains representative of a modern global movement. Despite its global presence, its large membership body has proved difficult to unite and thus susceptible to fracture. This is evidenced by the fractures that lead to the formation of more disruptive groups, such as ELF and the Animal Liberation Front. Causes for these fractures require further exploration and may signify the potential for similar activity in the global Anonymous collective.

Unlike the stated agenda of the environmental movement, the literature provides little background on Anonymous as a social movement since its agenda is vague and abstract. In attempting to identify the increased disruptive potential for Anonymous and similar hacktivist collectives, it is worthwhile to examine Anonymous's malleable agenda

---

53 *Emerging Cyber Threats Report 2013*, Georgia Institute of Technology, 2013, http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf.

54 Verizon, *2012 Data Breach Investigations Report*.

55 Brian Ault, "Joining the Nazi Party before 1930: Material Interests or Identity Politics?," *Social Science History*, 26, no. 2. (2002), 274, http://muse.jhu.edu/journals/social_science_history/v026/26.2ault.pdf, 273–310.

56 Roger Chapman, *Culture Wars: An Encyclopedia of Issues, Viewpoints, and Voices* (Armonk, New York: M.E. Sharpe 2009).

and determine whether this new social movement merits similar attention as previous global predecessors in the environmental movement. The recent actions of LulzSec, a smaller collective of Anonymous members incorporated from similar mimetic culture, conduced a multi-week "politically motivated ethical hacking" campaign against government and private sector networks in the name of Internet freedom and privacy.[57] Their efforts received global media attention as well as global attention from law enforcement who effectively dismantled the group. As a collective within Anonymous, LulzSec provides a unique opportunity to explore the praxis behind the Anonymous movement and whether the actions of LulzSec are representative of a more concerning move along the radical narrative. Additional academic research is required to more fully understand hacktivism as a new social movement and whether the cyber platform provides an increasing potential for more harmful disruptive actions like those briefly displayed by LulzSec.

D. METHODOLOGY

Research for this thesis will utilize qualitative case study analysis of activist movements and exploratory research to identify the vulnerabilities associated with increased Internet dependency. The assertion is that multiple case studies of historical activist movements compared to the current cyber activist movement will help identify causal factors for violence and how current activist movements may utilize the cyber venue to further their message. These methods were chosen because of the lack of academic research directly applicable to hacktivism as a social movement and the importance of cognitive praxis in identifying causal process in the activist movement. The assertion is that the study of activist movements in the terrestrial setting will provide a basis for better understanding the evolution potential for activism in the cyber domain. Case studies of the anti-Vietnam War movement and environmental movement will be compared with more recent actions involving cyber activists.

---

[57] Susan Watts, "Newsnight Online 'Chat' with Lulz Security Hacking Group," *BBC News*, June 24, 2011, http://www.bbc.co.uk/news/technology-13912836; Preet Bharara, United States of America v. Ryan Ackroyd, Jake Davis, Darren Martyn, Donncha O'Cearrbhail, U.S. Department of Justice, http://www.justice.gov/usao/nys/pressreleases/May13/HammondJeremyPleaPR/U.S.%20v.%20Jeremy%20Hammond%20S2%20Information.pdf.

The evidence sought by use of these methods is to gain an objective understanding of how hacktivist movements may evolve within the context of terrestrial social movements. The anti-war movement of the 1960s and early 1970s provides a unique historical perspective for review in that a number of activist movements resulted in splinter groups that engaged in disruptive and violent activity against persons and property. Case studies of the Students for a Democratic Society, Earth First! and Anonymous will provide a strong model for understanding how small segments of society express displeasure with social environment and the progression of such movements towards violent or disruptive action. All three movements emerged from linear or decentralized networks that formed collectivist forms of organization. Strong internal organizations emerged that, when challenged, resulted in splinter formations. However, the period of sustainment for each group differs and thus provides unique perspectives on failure and success. Earth First! splintered into a domestic terrorist group called the Earth Liberation Front (ELF), and this provides a unique study that, on the surface, appears to exist and survive in anonymity very similar to the hacktivist collective Anonymous. Both Anonymous and ELF are amorphous blobs capable of self-organization often triggered by random occurrences.

It is also important to recognize the differences in activist organizations and identify common or unique elements that enabled such civil rights organizations, such as the Students for a Democratic Society (SDS), to evolve into a revolutionary terrorist group known as the Weather Underground. The SDS, as a loose and non-hierarchical organization is very reflective of today's hacktivist collectives and may potentially reveal characteristics consistent with transformation. The selection of these movements is relevant for understanding the cognitive praxis behind social movements and for further understanding causal factors for splintering and development of potentially more disruptive groups within hacktivist movements. The data from these studies will be used to compare and contrast contextual conditions associated with the Anonymous collective.

It is difficult to formulate a true picture of hacktivism without considering the context from which previous social movements have evolved into direct action. Causal relationships and covariation will be loosely examined and compared to today's current

online activist collective with an eye towards better understanding the capability and potential threat posed by the modern cyber movement. By examining the structural and communicative properties for each group, this thesis will attempt to identify specific triggers and behavioral patterns that potentially lead to violent or disruptive behavior.

The cyber domain provides a unique opportunity for a small number of threat actors to project increased power. Thus, it can be surmised that the hacktivist, operating in the cyber environment, possesses the potential to cause serious disruption to government or private sector entities increasingly reliant on the Internet. To further examine this potential for harm, exploratory research will also be conducted to identify the vulnerabilities associated with increased dependence on the Internet and whether this potential wicked problem provides an adversarial advantage to the hacktivist.

E. THESIS OVERVIEW

This section introduces the structure of the thesis and, for each chapter, provides a short narrative concerning the focus and research to be addressed relative to the hypothesis. Each chapter was written to be largely self-contained and complete. To avoid excessive redundancy, lengthy information that is required in a later chapter of the thesis was occasionally referenced to an earlier chapter.

Chapter II will provide an in depth understanding of how the Internet has evolved and whether the current state supports the premise that individuals or groups with nefarious intent can utilize the Internet as a platform for disruption. This chapter will further explore the evolution of the Internet and how its original design allowed the web to be unwittingly coopted by nefarious actors.

Chapter III will examine the various type of threat actors on the Internet and the capabilities and motivations for each of these sources with specific detail given to the growing hacktivist threat group.

Chapter IV will examine the ideological and cognitive effects that the Internet has on the congruence of hacktivists and social discourse by examining the social science of collective behavior and its effects on cohesion, discourse, and fracture. Further

examination will be given to the Internet's additive effect of anonymity on individual and collective behavior to further understand the possible impact of hacktivism.

Chapter V will examine the origins and evolution of the 1960s student movement Students for a Democratic Society and the casual factors leading up to the formation of the violent splinter group called the Weather Underground. Analysis will focus on the impact of origin, structure, and communication on the decision-making process in the movement.

Chapter VI will explore the emergence of the 1970s environmental movement and subsequent creation of the direct action group Earth First! The group's structure and communication channels will be studied to possibly identify casual factors for the formation of more violent environmental groups such as the Earth Liberation Front.

Chapter VII will review the evolution of Anonymous as a web-based social movement and identify unique and distinctive characteristics that enabled the formation of more disruptive hacktivist clusters, such as LulzSec. Previous analysis will be utilized to identify possible similarities or indicators for increased disruption by Anonymous or other hacktivist groups.

Chapter VIII will identify key findings and effects that the Internet has on web-based social movements. The final chapter will also highlight the importance of understanding the contributing factors for disruption and the potential future implications for hacktivist movements.

II. NATURE OF THE THREAT

In order to realize the risk posed by web-based activists, it is first necessary to establish an understanding of how the Internet has evolved and whether the current state supports the premise that individuals or groups with nefarious intent can utilize the Internet as a platform for disruption. This chapter will further explore the evolution of the Internet and how its original design, though beneficial to its explosive growth, also allowed the web to be unwittingly coopted by nefarious actors. Once established, the chapter will examine how illicit appropriation of the web has heightened the nature of the threat posed by cyber dependency. Emphasis will be placed on the tools and malware commonly used by threat actors and how these tools are becoming increasingly available to amateur hackers and average citizens.

A. GROWTH OF THE INTERNET

The Internet has become an integral part of our existence in many parts of the world. Since the first email messages in 1970, the growth of the Internet has exploded and yet is considered to still be in its infancy. Today, cyberspace consists of millions of private, public, academic, government, military, and business networks. It connects everything from home computers and smartphones to government databases, telecommunication networks, and control systems used to operate the power grid.[58] In essence, the Internet has become a "global commons"; it exists almost everywhere, open to anyone, allowing its inhabitants to move across it with ease and at ever-increasing speeds.[59] However, America's interconnectivity and interdependence on the Internet has become a wicked problem. According to Cisco, in 2008, the number of "things"

[58] Howard A. Schmidt, "Cyber Threats and Cyber Doman: Implications of National Security," Codenomicon, accessed July 17, 2014, http://www.codenomicon.com/news/editorial/Howard%27s%20Interview%20for%20Maanpuolustuslehti.pdf, 40–43.

[59] Issac R. Porche III, Jerry M. Sollinger, and Shawn McKay, *A Cyberworm That Knows No Boundaries*, Occasional Paper (Santa Monica, CA: RAND Corporation, 2011), http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf, 2.

connected to the Internet exceeded the number of people on earth and is projected to reach 50 billion by the year 2020.[60]

In his 2013, paper about cyber security and critical infrastructure, Dave Clemente noted that cyberspace has become so deeply embedded into America's sectors that it is indistinct amongst other critical infrastructure components such as energy, water, and communication. He describes cyberspace as a "thin layer or nervous system running through all other sectors, enabling them to function and interconnect."[61] However, America's reliance upon this interconnectivity is also its Achilles heel and can be exploited by anyone with savvy technical capabilities and access to the web. In October 2012, U.S. Defense Secretary Leon Panetta warned that threat actors have already gained access to some of America's critical control systems that run chemical, electric, and water systems with the intent to "cause panic, destruction and loss of life."[62] According to MIT's *Technology Review*, this threat scenario is plausible because of the outdated technology used to operate critical infrastructure and states that some of the software used to operate critical infrastructure has not been updated since its initiation.[63]

Panetta's comments are reflective of the actions of ideologically based hackers who utilize their skills and web-based tools for disruptive means in order to elevate attention to an issue or, in more limited circumstances, force policy change. The threat posed by hacktivists and other malicious actors on the web results from mainly three things: the ubiquity of Internet-connected devices, the global reliance on cyberspace, and the inadequacy of cyber security.[64] The interconnectivity between the billions of "things"

---

60 "Cisco Visualization, The Internet of Things," Cisco, accessed March 28, 2014, http://share.cisco.com/Internet-of-things.html

61 Dave Clemente, *Cyber Security and Global Interdependence: What Is Critical?* (London, United Kingdom: Chatham House, 2013), http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf

62 Jim Miklaszewski and Courtney Kube, "Panetta: Cyber Intruders Have Already Infiltrated U.S. Systems," *U.S. News*, October 11, 2012, http://usnews.nbcnews.com/_news/2012/10/11/14376572-panetta-cyber-intruders-have-already-infiltrated-us-systems?lite\.

63 Geoffrey Ingersoll, "Here's Why the U.S. is Incredibly Vulnerable to Cyber Attacks," *Business Insider*, October 15, 2012, http://www.businessinsider.com/heres-why-the-us-is-incredibly-vulnerable-to-cyber-attacks-2012-10.

64 Clemente, *Cyber Security and Global Interdependence*.

suggests that even the slightest web disturbance can result in a cascading effects possibly resulting in a disproportionate threat or response. According to a recent report from McKinsey & Company, a global management consulting firm, "the global economy is still not sufficiently protected against cyber attacks—and it is getting worse" adding the "risk of cyber attacks could decelerate the pace of technology and business innovation with as much as $3 trillion in aggregate impact."[65] In March 2013, a simple targeted attack against the web servers of Spamhaus, an anti-spam company in the United Kingdom, resulted in a global ripple effect that slowed down or limited access to Internet sites and servers around the world.[66] Very large attacks like this are easily accomplished and usually originate from a number of sources. This particular attack, called a distributed denial of service or "'DDoS,'" directed Internet traffic to Internet address for Spamhaus' web servers effectively creating a tidal wave that overwhelmed the network. Since Spamhaus was responsible for filtering email messages for nearly 80 percent of the Internet's spam or junk mail messages, the DDoS attack had a significant effect on Internet traffic.[67] The sources of attack traffic can be a group of individuals working together such as the hacktivist collective Anonymous or a smaller number of persons with access to a number of compromised computers. These techniques will be discussed later in this chapter. To understand how all this is possible, a closer examination of the cyber domain is warranted.

B. ARCHITECTURE BY DESIGN

America's reliance on cyber networks stands in stark contrast to its lack of cyber security. Cyber networks, including those that comprise of critical infrastructure, contain vulnerabilities, which can be exploited to access critical information or to disrupt

---

65 Brian Taylor, "Cyberattacks Fallout Could Cost the Global Economy $3 Trillion by 2020," TechRepublic, February 20, 2014, http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/.

66 "Cyberattack on Anti-Spam Group Spamhaus Has Ripple Effects," *CBS News*, March 27, 2013, http://www.cbsnews.com/news/cyberattack-on-anti-spam-group-spamhaus-has-ripple-effects/.

67 Matthew Prince, "The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)," *Cloud Fare* (blog), March 20, 2013, http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho.

operations.[68] In response to a growing need to share research and communication between isolated computer nodes, the U.S. Defense Advanced Research Projects Agency (DARPA) initiated a research program to investigate techniques and technologies for interlinking the isolated networks. By developing communication protocols (Transmission Control Protocol (TCP) and Internet Protocol (IP)) for networked computers to talk with each other, DARPA developed a communication backbone today known as the Internet.[69] This design embodied a key underlying technical idea, namely that of open architecture networking, an unsecure platform for continuous design innovation. Thus, as an open architecture, any network could be "selected freely by a provider and made to interwork with the other networks through a meta-level 'Internetworking Architecture.'"[70]

Joseph Kizza, author of the book *Computer Network Security and Cyber Ethics*, describes an ill-conceived cyber infrastructure developed without a clear set of blueprints. Infrastructure growth was reactive in response to the changing needs of developing communications between computing elements.[71] This "open architecture protocol" gave birth to the computer industry and the eventual rapid growth of the Internet. Much like the application or "apps" platform for smartphones, open protocol invites many architects, some of whom are interested in exploiting this architecture for a variety of less productive or nefarious reasons, including pranks, financial gain, and activism. According to Vinton Cerf, one of the "fathers of the Internet," Internet protocols were published openly to be used without licensing or approval.[72] Hoping to grow the Internet organically through independent communication, Cerf intended that new applications would be implemented without permission from Internet service providers. However,

---

68 Schmidt, "Cyber Threats."

69 "A Brief History of the Internet & Related Networks," Internetsociety, accessed July 17, 2014, http://www.internetsociety.org/Internet/what-Internet/history-Internet/brief-history-Internet-related-networks.

70 Ibid.

71 Joseph Migga Kizza, *Computer Network Security and Cyber Ethics*, 2nd ed. (Jefferson, NC: McFarland & Company 2006), 84.

72 Vinton G. Cerf, "The Open Internet and the Web," CERN, April 15, 2014, http://home.web.cern.ch/cern-people/opinion/2013/04/open-Internet-and-web.

open connectivity meant that "parts of the Internet could attack other parts" by infecting computers and network servers with malware and Botnets utilized to "generate spam, launch denial of service attacks and to conduct corporate and government espionage."[73]

Today the cyber domain operates in an atmosphere of trust that enables communications through a series of partially opened windows connected via a "three-way handshake."[74] Computers exchange information via a formal handshake between clients and servers that, once established, leaves a small window open for continued information exchange or communication between the trusted partnerships. Hackers undermine this trust relationship and the open window by creating a three-way handshake that enables them to exploit this vulnerability. Thus, the Internet's communication network becomes only as good as its "weakest hardware link and its poorest network protocol."[75] This ill-fated arrangement opens the cyber ecosystem up to a number of threats whose temporary fixes are a series of software patches that do not address the actual issue of the Internet's original architecture design.

C. UNINTENDED CONSEQUENCES

As computer technology has advanced, U.S. critical infrastructures, such as energy, finance, and telecommunications, have increased their dependence on cyber systems to carry out operations and to process, maintain, and report essential information.[76] Similarly, federal agencies and state and local governments increased their use of information and data systems also becoming entwined in the cyber ecosystem. The General Accountability Office (GAO), in recognition of this increased dependence on computer systems and the systems that support critical infrastructures, highlighted cyber critical infrastructure protection (CIP) as a continuing concern. Among the many risks to the cyber CIP, the GAO noted the ease of obtaining and using hacking tools, the steady

---

[73] Ibid.

[74] Kizza, *Computer Network Security and Cyber Ethics*, 70.

[75] Ibid., 85.

[76] U.S. Government Accountability Office, *Protecting the Federal Government's Information Systems and Nation's Cyber Critical Infrastructures*, 2013, http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study.

advance in the sophistication of attack technology, and the emergence of new and more destructive attacks as high concern.[77]

According to Deibert and Rohozinski, cybercriminals exploit the "relative anonymity offered by the Internet, as well as the absence of harmonized national laws defining cybercrime, to circumvent or avoid prosecution."[78] Traditional criminals look for low-hanging fruit or easy targets, much like the unattended home with the open front door. Today, because of the previously described architectural flaws, the global e-economy, and jurisdictions with poorly functioning or nonexistent Internet laws, criminals have moved online out of the reach of authorities in jurisdictions where such activities are clearly criminalized.[79] The discouraging result is that staying a step ahead of cybercriminals is much more difficult than staying ahead of the traditional criminal actor.

However, as cybercriminals have become more adept at using the Internet for crime, so too have governments and law enforcement become more adept at detecting their activities. Those wishing to remain engaged in unlawful or subversive activities have been forced to develop new safe havens from which to continue their deeds. In addition to the criminals, the persistent plight of dissidents, such as the Nepalese bloggers who are being arrested by the government for "misuse of democratic freedoms to attack state interests" or civil suits against music file sharers have exacerbated the cry for Internet freedom and the right to anonymity.[80]

Today, cybercriminals achieve anonymity via sophisticated encryption programs. To prevent unauthorized access to data or communication, software suites use sophisticated encryption algorithms. The software rearranges bits of data into complex

---

77 Ibid.

78 Ronald Deibert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald Diebert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, 123–49. Cambridge, MA: MIT Press, 2008), 131.

79 Ibid.

80 "Third Blogger Arrested in Less than a Month," *Reporters without Borders*, June 17, 2013, http://en.rsf.org/vietnam-blogger-and-former-party-official-17-06-2013,44801.html.

puzzles that requires a decryption keys to decipher. The private key (originator) and public key (authorized recipient) utilize an *infinite* number of alpha and numeric sequences to form an encryption chain that is extremely secure and resilient to even the most powerful computer processors.[81] Various applications of this technique are available via the web, such as Pretty Good Privacy or PGP, which can be used to secure email, texts, files, and other forms of Internet communications.[82] Encryption technologies continue to evolve and now use layers of encrypted chains each requiring authentication before allowing access to the next encrypted layer.

One such commonly used and free encrypted layer program is known as Tor, short for The Onion Router. Tor enables online anonymity by directing Internet traffic through a global network of more than five thousand relays.[83] Tor uses layers of servers to separate computer users from the websites they visit to hide a user's location.[84] This expansive network conceals a user's location or usage from anyone conducting network surveillance or traffic analysis. Tor is intended to protect the personal privacy of users and their ability to conduct confidential business by keeping their Internet activities from being monitored. The National Security Agency characterized Tor as "the King of high secure, low latency Internet anonymity."[85]

D. MARKET FOR WEAPONS

Though Tor and other encryption programs have many legitimate uses for business transactions and personal communications, these same technologies are being appropriated for illicit use. A 2014 RAND report on cybercrime revealed that online black markets are growing in size and complexity and can be more profitable than the

---

81 Jeff Tyson, "HowStuffWorks 'Public Key Encryption,'" HowStuffWorks, accessed August 1, 2014, http://computer.howstuffworks.com/encryption3.htm.

82 "Encryption Software," Symantec, accessed August 1, 2014, http://www.symantec.com/products-solutions/families/?fid=encryption.

83 "TorStatus—Tor Network Status," accessed July 17, 2014, http://torstatus.blutmagie.de/.

84 Jonathan D. Glater, "Privacy for People Who Don't Show Their Navels," *New York Times*, January 25, 2006, http://www.nytimes.com/2006/01/25/technology/techspecial2/25privacy.html?_r=0.

85 "Tor: 'The King of High-Secure, Low-Latency Anonymity,'" *The Guardian*, October 4, 2013, http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-Internet-anonymity.

illegal drug trade.[86] This is suggestive of the increasing number of cyber threat actors gaining access to sophisticated cyber weapons and "poses a formidable challenge and an increasing threat to businesses, governments, and individuals operating on the digital world."[87] The flourishing black market offers the ability for threat actors to buy or rent cyber tools that can penetrate just about any computer system in use today, as well as the infrastructure to carry out even large-scale operations.[88] Most concerning in RAND's assessment is that "almost any computer-literate person" can gain access to the cyber black markets and its catalog of tools and malware. Internet sites such as YouTube and Google provide easy access to a number of videos describing how to use hacker toolkits to break into websites or steal bank account login credentials.[89] The popularity of these so-called black markets has enabled "anybody to buy a gun" elevating concern for security experts.[90]

A diverse number of malicious products and services can be found on the web. A review of security data reveals the following most commonly acquired techniques utilized to conduct cyber attacks: viruses, worms, and denial of service attacks.

E. COMPUTER VIRUSES/WORMS

Computer viruses refer to usually small pieces of software that attach themselves to email or other files that, when open, enable access into an unwitting computer system or network. The replicating nature of viruses enable them to quickly create harm to the infected system by either corrupting the affected drive or gaining access to protected

86 Lillian Ablon, Martin Libicki, and Andrea Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, CA: RAND Corporation, 2014).

87 Ibid.

88 *Hearing to Receive a Briefing on Cybersecurity Threats in Review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program, United States Senate, Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities*, 113th Cong. (2013) (testimony of Kay R. Hagen, Mandia, Kevin, and Bejtlich Richard), https://www.hsdl.org/?view&did=736724.

89 MatzHKR, "Hacking Tools 6.0," YouTube Video, October 1, 2009, http://www.youtube.com/watch?v=UGGalB0bc_.

90 Harvey Rishikof and Bernard Horowitz, *Shattered Boundaries: Whither the Cyber Future* (Calgary, Alberta, Canada: Centre of Military and Strategic Studies, 2012).

information. Properly engineered viruses can have devastating effects usually resulting in loss of productivity.

In August 2012, the Saudi Arabian Oil Company, also known as Saudi Aramco, was targeted by a group of hackers that managed to infect approximately 30,000 workstation computers operating within the company's network.[91] Utilizing a virus designed to erase or wipe data from Saudi Aramco's affected network hard drives, the hacker(s) intended to disrupt the company's crude and oil gas supplies "potentially causing devastating effects to the global market."[92] Based in Saudi Arabia, Saudi Aramco is the world's largest oil and gas producer and one the world's most valuable companies with an estimated worth of $10 trillion.[93] Yet despite its worth and value as a critical infrastructure component, Saudi Aramco was still victimized by a group of "skillful amateurs" who deployed a self-replicating computer virus available via the Internet.[94] An "anti-oppression hacker group" named Cutting Sword of Justice claimed responsibility for the attack stating they were "fed up of crimes and atrocities taking place in various countries around the world."[95] The virus was used to propagate a political message and its effects on Saudi Aramco's network were felt for more than two months. The Saudi Aramco attack is regarded as one of the most destructive acts of computer sabotage on a company to date.[96]

---

91 Camilla Hall and Javier Blas, "Aramco Cyber Attack Targeted Production," *Financial Times*, December 10, 2012, http://www.ft.com/cms/s/0/5f313ab6-42da-11e2-a4e4-00144feabdc0.html#axzz3Af5d25Vk.

92 Ibid.

93 Charles Orton-Jones, "Stop the Press! Apple Is NOT the World's Most Valuable Company," LondonlovesBusiness.com, August 21, 2012, http://www.londonlovesbusiness.com/business-news/finance/stop-the-press-apple-is-not-the-worlds-most-valuable-company/3250.article.

94 Kelly Jackson Higgins, "Destructive Attacks on Oil and Gas Industry A Wake-Up Call," DarkReading, September 23, 2013, http://www.darkreading.com/attacks-breaches/destructive-attacks-on-oil-and-gas-industry-a-wake-up-call/d/d-id/1140525?.

95 A Guest, "Untitled," Pastebin.com, August 15, 2012, http://pastebin.com/HqAgaQRj.

96 Nicole Perlroth, "Cyberattack on Saudi Oil Firm Disquiets U.S.," *New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0.

Worms are similar to a virus; however, worms are standalone software and do not require a host program or human help to propagate.[97] Computer worms have the capability to replicate and travel quickly throughout the Internet with potentially devastating effects. The replicating worm often overwhelms the affected system causing it to stop responding to web traffic or shut down. The famous Code Red worm swept across computers worldwide in 2001 by exploiting a flaw in one of Microsoft's web servers successfully bringing down a number of private and government websites to include the whitehouse.gov site.[98] However, the famous Stuxnet worm is perhaps the most alarming and most ominous sign of the increasing sophistication and dangerousness of cyber based weapons.

The Stuxnet worm was a **zero-day exploit** designed to target vulnerabilities in software that have not yet been discovered by their manufacturers enabling the worm to activate at a designated time and date.[99] Hackers exploit these vulnerabilities or "holes" before a vendor is aware of the issue and fixes the problem. The subsequent attack is known as a zero-day attack and can include infiltrating malware, spyware, or allowing unwanted access to user information.[100] Stuxnet, believed to be a covert effort by one or more nation states, was inserted into Iran's industrial control systems for its nuclear enrichment program via an identified vulnerability in the Microsoft Windows software used to operate the system's hardware.[101] Once activated, the worm collected information about the operation of the industrial systems and prompted the fast-spinning centrifuges

---

97 Cisco Systems, "What Is the Difference: Viruses, Worms, Trojans, and Bots?," Cisco, accessed July 18, 2014, http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html.

98 Sharon Weinberger, "Top Ten Most-Destructive Computer Viruses," *Smithsonian*, March 19, 2012, http://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/.

99 Shane Harris, "Black Market for Malware and Cyber Weapons Is Thriving," *Foreign Policy*, March 25, 2014, http://complex.foreignpolicy.com/posts/2014/03/24 /black_market_for_malware_and_cyber_weapons_is_thriving.

100 "What Is a Zero-Day Vulnerability?" Security News, accessed July 18, 2014, http://www.pctools.com/security-news/zero-day-vulnerability/.

101 David E. Sanger, "Obama Ordered Wave of Cyberattacks gainst Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2&partner=rss&emc=rss&.

to tear themselves apart.[102] By targeting industrial control systems, Stuxnet became the first computer virus to be able to wreak havoc in the physical world.[103]

As is the problem with most malware, once deployed, Stuxnet quickly became available to anyone on the web creating a possible proliferation problem that will make it easier for terrorist organizations and other politically motivated actors to develop such capabilities in the future.[104] According to Eric Rosenbach, the U.S. deputy assistant secretary of defense for cyber policy, the growing black market for malware, specifically zero-day vulnerabilities, is allowing almost anyone to buy the means to launch destructive cyber-attacks to include against U.S. industrial control systems.[105]

F. DISTRIBUTED DENIAL OF SERVICE

Distributed denial-of-service (DDoS) have been utilized by hackers for decades and are a principal tool in the hacktivist toolkit. The first well-known DDoS attack occurred against the University of Minnesota in August 1999.[106] This two-day attack involved flooding servers with data packets originating from over 1,000 compromised computers. The computers were used at different times to attack a single server at the University of Minnesota resulting in denied access to a very large university network.[107]

Since this initial attack, DDoS attacks have become more sophisticated and have evolved to include a number of distinct characteristics that include flood attacks, mail bombing, permanent denial-of-service attacks, and distributed denial-of-service (DDoS)

---

[102] David Kushner, "The Real Story of Stuxnet," IEEE Spectrum, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[103] "Stuxnet Virus: Battling the Stuxnet Worm," Symantec, accessed July 18, 2014, http://www.symantec.com/en/uk/theme.jsp?themeid=stuxnet.

[104] Paul K. Kerr, John Rollins, and Catherine Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Washington, DC: Congressional Research Service, 2010), https://cyberwar.nl/d/R41524.pdf.

[105] Stew Magnuson, "Growing Black Market for Cyber-Attack Tools Scares Senior DOD Official," *National Defense Magazine*, February 22, 2013, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1064.

[106] Philip Boyle, "SANS: Intrusion Detection FAQ: Distributed Denial of Service Attack Tools: Trinoo and Wintrinoo." Sans.org, accessed March 28, 2014, http://www.sans.org/security-resources/idfaq/trinoo.php.

[107] Rik Farrow, "Distributed Denial of Service Attacks," Chinese-School.netfirms.com, accessed March 28, 2014, http://chinese-school.netfirms.com/computer-article-denial-of-service.html.

attacks. In the case of a denial of service attack, the attacker installs software onto unwitting computer for the purpose of co-opting the computer to be employed as one of many "zombie" computers in future network attacks. The owner of the coopted computer is usually unaware of this compromise.[108] Once an army of zombie computers has been employed, the attacker sends a series of large data packets to a targeted computer system or network. The targeted system becomes overwhelmed and either reboots itself, thus taking it offline, or unable to receive legitimate information requests.[109] The attacker, in using a series of compromised and usually unwitting computers, has not only formed a small army of attack computers but has also derived the benefit of anonymity making it difficult to identify the source of the attack. (See Appendix)

This use of intermediary computers presents a two-fold problem. Intermediaries make attribution difficult since the zombie computers effectively shield the identity of the attacker. Second, by using intermediaries, hackers can form an army of zombie computers, otherwise known as botnets, to create a large-scale attack with little or no effort.[110]

In 2007, Russian hacktivists conducted a sophisticated DDoS attack against the country of Estonia as part of a protest action against the country's decision to relocate a bronze statue that honored Russia's deceased World War II veterans. Cognizant of Estonia's heavy reliance on the Internet and online services, hackers conducted a virtual invasion of Estonia via a series of DDoS attacks against Estonian banking and government sector networks. These attacks lasted for a period of approximately three weeks, effectively disrupting banking and government communication. According to the *New York Times*, hacktivists flooded Estonian networks with a data load equivalent of the entire Windows XP operating system every six seconds for 10 hours.[111] Hannabank,

---

[108] Ibid.

[109] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Distributed Denial of Service Attacks," *The Internet Protocol Journal* 7, no. 4 (2004): 13–35, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/ipj_7-4.pdf.

[110] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, accessed March 29, 2014, http://www.iar-gwu.org/node/65.

[111] Cristen Conger, "Could a Single Hacker Crash a country\u0027s Network?," HowStuffWorks, August 12, 2009, http://computer.howstuffworks.com/hacker-crash-country-network2.htm.

Estonia's largest bank and one of the prime targets of the attack, lost revenue in excess of one million dollars due to disrupted credit card and automatic teller machine transactions.[112] The parliamentary email server and the IT capabilities of several government ministries were disabled, paralyzing the state's ability to effectively respond. Howard Schmidt, the White House cyber-security czar, acknowledged the seriousness of these attacks stating that the high tech nation of Estonia had "basically been brought to their knees."[113] Although no critical infrastructure was permanently disabled during the attack, the events "consumed the affairs of an entire government and drew the attention of the world."[114]

Today, a sophisticated DDoS tool known as the Low Orbit Ion Cannon (LOIC) has become a favorite of the hacktivist group Anonymous. The tool, originally created to perform witting stress tests of computer networks, and now readily available via the web, has been altered to enable a limited number of hacktivists to direct and control the attack.[115] By enabling a programmed option called the "Hive Mind," members wittingly and sometimes unwittingly enable their computer to be used to attack any target. Anonymous has also altered this program to be utilized via select Twitter accounts eliminating the extra step of downloading the tool to a computer.[116] By clicking on a link on Twitter, users submit enable their computer to be used for targeted DDoS attacks. Use of such tools is a crime punishable by law in the United States and other western nations.[117]

---

[112] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49–60.

[113] Larry Greenemeier, "Estonian Attacks Raise Concern over Cyber 'Nuclear Winter,'" InformationWeek.com, May 24, 2007, http://www.informationweek.com/estonian-attacks-raise-concern-over-cyber-nuclear-winter/d/d-id/1055474?

[114] Jacob Silverman, "Could Hackers Devastate the U.S. Economy?," HowStuffWorks, June 25, 2007, http://computer.howstuffworks.com/die-hard-hacker1.htm.

[115] Vanja Svajcer, "Hacker Toolkits Attracting Volunteers to Defend WikiLeaks," NakedSecurity, December 9, 2010, http://nakedsecurity.sophos.com/2010/12/09/low-orbit-ion-cannon-the-tool-used-in-anonops-ddos-attacks/.

[116] Christina Warren, "How Operation Payback Executes Its Attacks," Mashable, December 9, 2010, http://mashable.com/2010/12/09/how-operation-payback-executes-its-attacks/.

[117] Graham Cluley, "Are DDoS (Distributed Denial-of-Service) Attacks against the Law?," Naked Security, December 9, 2010, http://nakedsecurity.sophos.com/2010/12/09/are-ddos-distributed-denial-of-service-attacks-against-the-law/.

G. CONCLUSION

The Internet is just one of many technologies hijacked for nefarious purposes. Zyklon B, a chemical originally designed as pesticide and disinfectant was notoriously utilized to kill scores of innocents in the Nazi death camps during World War II. Albert Noble invented dynamite to assist with mining and building thus making the expansion rail in the U.S. more efficient. Noble's invention has since been used as a weapon of war and terror and famously used to kill 38 people on Wall Street in 1920.[118] More recently, three-dimensional printing technology has been used to create both medical implants and untraceable firearms. Cyber attacks are continuing examples of the misuse of tools for nefarious purposes. The faulty infrastructure of the Internet is compounded by the now almost immediate availability of sophisticated cyber weapons that, with the right motivation, could cause significant harm to America's critical infrastructure. It is often stated that the cyber threat is overblown and is part of a new industrial complex; however, the few examples discussed in this chapter are testimonial to the real and significant threat lurking in the cyber domain. Recognizing this potential, the National Intelligence Council issued a report in 2004 that noted "today individual PC users have more capability at their fingertips than NASA had with the computers used in its first moon launches."[119] With little investment, and the proper motivation, a threat actor could purchase the hardware and software necessary to disrupt critical U.S. infrastructure. However, weapons are not born of themselves; they require a person or persons to contrive of their use. The next chapter will identify the types of threats actors found on the web and delve further into specific hacktivist profiles.

---

[118] Alan Bellows, "Terror on Wall Street," Damninteresting.com, May 14, 2007, http://www.damninteresting.com/terror-on-wall-street/.

[119] Dan Caldwell and Robert E. Williams, Jr., *Seeking Security in an Insecure World* (New York, New York: Rowman & Littlefield Publishers 2006), 92.

III. THREAT ACTORS

The concern regarding the proliferation of cyber-based weapons is equally matched by the proliferation of threat actors willing to use these weapons. Motivations behind such uses are many and are reflected in the number of daily cyber-based threats that confront the U.S. each day. These threats consist of both targeted and untargeted attacks from a variety of threat actors, such as criminal groups, terrorists, and hacktivists.[120] The sources of these threats vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include financial gain or, in the case of terrorism and hacktivism, political influence through disruption. To accomplish these goals, threat actors utilize a number of effective cyber based tools and techniques that are readily available via the web. Emboldened by the anonymity of the Internet, attackers utilize social media and secure communication platforms to access likeminded folks with a variety of skillsets. Hackers are often motivated, in part, by their invisibleness; however, their true motivations can be varied and complex.[121] This chapter will examine the various type of threat actors on the Internet and the capabilities and motivations for each of these sources with specific detail given to the growing hacktivist threat group.

A. CRIMINAL HACKERS

Hackers enjoy the thrill of being able to peek into company servers and seek restricted information about a company or government agency. Although these hackers may lack malicious intent, at least initially, their actions are undoubtedly criminal. The lack of criminal intent also does not lessen the dangerousness of their actions, rather, it distinguishes them from a more sophisticated network of criminal hackers motivated by financial gain. In fact, the thrill seeking hacker is often glorified as one who is providing a greater good by exposing security flaws in networked systems. This is not unusual and consistent with hacker discourse that suggests exposing the naked emperor is a public

120 Gregory C. Wilshusen, *Cybersecurity: Threats Impacting the Nation* (Washington, DC: U.S. Government Accountability Office, 2012), http://www.gao.gov/assets/600/590367.pdf.

121 "Motivations of a Criminal Hacker," Microsoft, accessed August 6, 2014, http://msdn.microsoft.com/en-us/library/cc505924.aspx.

service and consistent with hacker ethos. Such actions have given birth to the term "ethical hacker" and are used to justify what is otherwise a criminal act. Much like the activist hacker, so-called ethical hackers engage in criminal acts to further a personal agenda. Some, termed "white hats," penetrate computer systems to raise awareness of systems flaws allowing the system owners to repair the holes before a malicious attack takes place.[122]

Not everyone is aligned with the concept of "ethical" hacking since the actions of these alleged whistleblowers are often illegal. Perhaps the biggest and most infamous example of this divergence is represented by the actions of Edward Snowden, a NSA contractor who singlehandedly exposed some of the country's most sensitive intelligence programs to the world. Disenchanted with the extent of the U.S. government's extensive meta data collection and surveillance efforts, one he termed "intent on making every conversation and every form of behavior in the world known to them." Snowden, an experienced information technology (IT) security specialist, accepted an assignment to an NSA post in Hawaii with the intention of exposing the agency's top secret surveillance programs.[123] A hacker of a different sort, Snowden, using his "authority" as an IT security specialist, convinced fellow NSA co-workers to provide him with their closely held passwords thus falling victim to a commonly used hacker technique called social engineering.[124] Over the next few weeks, Snowden proceeded to download thousands of classified documents containing information on the surveillance programs of the U.S., the United Kingdom, and other countries involved in joint surveillance operations. Using PGP encryption tools, Snowden contacted a number of world media outlets and activist groups and provided them with thousands of the classified documents causing

---

[122] Margaret Rouse, "What Is White Hat?" *TechTarget*, June 2007, http://searchsecurity.techtarget.com/definition/white-hat.

[123] Luke Harding, "How Edward Snowden Went from Loyal NSA Contractor to Whistleblower," *The Guardian*, January 31, 2014, http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract.

[124] Michael Isikoff, "Exclusive: Snowden Swiped Password from NSA Coworker," *NBC News*, February 12, 2014, http://www.nbcnews.com/news/investigations/exclusive-snowden-swiped-password-nsa-coworker-n29006.

tremendous harm to the U.S. government's national security programs.[125] In a recent ruling concerning metadata collection of telephone records, a federal court ruled that the NSA program was "almost certainly unconstitutional."[126] Snowden claims to be a patriot who upheld his oath to defend the U.S. Constitution, a constitution he claims was being violated on a massive scale by the U.S. government.[127] The *New York Times* went so far as to call him a patriotic whistle-blower who has done a great service to the country.[128]

Others see Snowden as a traitor who may have caused irreparable harm to U.S. national security and suggest that the damage done to national security does not justify his actions.[129] Regardless of one's position, Snowden, using his hacking skills and the power of the Internet, effectively elevated awareness of a significant national program and caused U.S. policymakers to reexamine the extent of the U.S. government's metadata collection and surveillance programs.

Unlike Snowden, other criminal hackers are motivated by the prospect of a big payday. As discussed in the previous chapter, many cyber criminals have adapted their methods and are increasingly using cyberspace to gain monetizable information and exploit our nation's financial payment systems to engage in fraud and illicit activities. The widely reported payment card data breaches of Target, Niemen Marcus, White Lodging, and other retailers are just recent examples of this trend.[130]

---

125 Suzanna Andrews, Bryan Burrough, and Sarah Ellison, "Snowden Speaks: A Vanity Fair Special Report," *Vanity Fair*, May 2014, http://www.vanityfair.com/politics/2014/05/edward-snowden-politics-interview.

126 Ellen Nakashima and Ann E. Marimow, "Judge: NSA's Collecting of Phone Records Is Probably Unconstitutional," *The Washington Post*, December 16, 2013, http://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html.

127 Ibid.

128 The Editorial Board, "Edward Snowden, Whistle-Blower," *New York Times*, January 1, 2014, http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html.

129 "Transcript of President Obama's Speech on NSA Reforms," *NPR*, January 17, 2014, http://www.npr.org/blogs/itsallpolitics/2014/01/17/263480199/transcript-of-president-obamas-speech-on-nsa-reforms.

130 Gregory Wallace, "Target and Neiman Marcus Hacks: The Latest," *CNN Money*, January 13, 2014, http://money.cnn.com/2014/01/13/news/target-neiman-marcus-hack/.

The low risk, high reward environment on the web has made it an attractive environment for various types of criminal groups. According to Dr. Tatiana Tropina, Senior Researcher at the Cybercrime Institute in Cologne, Germany, organized criminal groups are attracted to the web because of the "the easiness of communication, anonymity, and the accessibility of tools for illegal operations."[131] High consequence cyber crimes are not accomplished by isolated individuals; rather it is typically a transnational network of criminal associates, each with their own specialized role, engaging in a multi-national conspiracy to obtain valuable information, monetize this information through fraud and other illicit activities, and launder their criminal proceeds. These associates are organized within "multi-skilled, multifaceted virtual criminal networks centered on online meetings."[132] Much like other online collectives, such as Anonymous, the criminal networks rarely meet each other in person but rather organize and conspire in virtual chat rooms or message boards created solely for the purpose of exchanging and selling stolen goods or data on the web. Leading members of the group divide the criminal actors into different segments that are reflective of the member's skillset: hackers, money launderers, malware developers, resellers, etc., usually all unknown to each other. These actors are joined together to carry out lucrative criminal acts.

In 2004, one such group called Shadowcrew evolved into a successful international organization of over 4,000 members skilled in hacking, identity theft, data exfiltration, and the fencing of ill-gotten wares on the web. Primarily focused on hacking financial institutions for financial data, such as credit card and bank account information, members of the group skilled in hacking and exfiltration would post account information on the group's message boards for further distribution to paying customers or group members willing to replicate the accounts for retail purchases and money withdrawals. Skilled money launderers transfer the ill-gotten proceeds into personal bank accounts, with everyone involved in the operation receiving a percentage of the proceeds. After

131 Tatiana Tropina, "Cyber Crime and Organized Crime," *F3 Magazine*, accessed August 3, 2014, http://f3magazine.unicri.it/?p=310z.

132 Ibid.

obtaining the cooperation of one of the group's members, the U.S. Secret Service disrupted the criminal network and indicted over two dozen members of the group for criminal activity associated with their operation. It is estimated that in less than two years, the group stole over 1.7 million credit cards for a profit of more than $ 4 million.[133]

Using similar structure and tactics, a group of cyber thieves joined forces for a series of operations dubbed "Unlimited Operation." During a two-year period from 2012–2013, organized hackers gained access to a number of credit card processors that enabled them to not only steal prepaid credit card data but also manipulate the servers to eliminate the withdrawal limits on the accounts. Once inside, the group obtained the support of small cells of street runners or cashers from around the world, who after receiving the counterfeited credit and debit cards associated with the breach, withdraw an unlimited amount funds from automated teller machines around the world. In less than two years, the group conducted tens of thousands of transactions for a profit of more than $40 million.[134] The U.S. Attorney's Office for the Eastern District of New York attributed the success of these attacks to the group's speed and meticulous planning, surgical precision, and the global nature of the cybercrime organization.[135]

According to Verizon, 75 percent of all data breaches in 2012 were motivated by financial gain making criminal hacking activity the most predominate form of illicit activity on the web.[136] In 2013, criminal hackers breached Target's payment system stealing payment information for approximately 70 million of its customers resulting in a

---

[133] Sarah Hilley, "Case Analysis of the Shadowcrew Carding Gang," Bank Info Security, April 3, 2006, http://www.bankinfosecurity.com/case-analysis-shadowcrew-carding-gang-a-136/op-1.

[134] Dan Goodin, "How Hackers Allegedly Stole 'Unlimited' Amounts of Cash from Banks in Just Hours," Ars Technica, May 9, 2013, http://arstechnica.com/security/2013/05/how-hackers-allegedly-stole-unlimited-amounts-of-cash-from-banks-in-just-hours/.

[135] United States Attorney's Office, Eastern District of New York, "Eight Members of New York Cell of Cybercrime Organization Indicted in $45 Million Cybercrime Campaign," U.S. Department of Justice, May 9, 2013, http://www.justice.gov/usao/nye/pr/2013/2013may09.html.

[136] Verizon, *2013 Data Breach Investigations Report*.

46 percent reduction in its fourth quarter profit alone.[137] Experts believe Target will ultimately lose between $100–250 million as a result of this one breach.[138] Such costs do not address the requisite legal fees and damage control costs to protect its brand. Web based anonymity combined with difficult transnational enforcement efforts will continue to benefit financially motivated cyber criminals.

B. NATION STATE/ADVANCED PERSISTENT THREAT

Nation states conduct cyber hacking activity to engage in information-gathering and espionage activities.[139] These acts of espionage are necessary to further develop offensive plans for sabotage in times of conflict. According to Wilshusen, persistent state use of cyber tactics against the United States enhances the warfare doctrines for nation perpetrators who are otherwise powerless against the U.S. military.[140] According to a report by the GAO, such capabilities enable a single entity to have a significant and serious impact by disrupting critical U.S. infrastructure and networks that support military power.[141]

Nations, such as China, also utilize cyber tools to steal valuable trade secrets, intellectual property data, and confidential business strategies of U.S. based companies. Such acts by China and other state actors drain America of its competitive advantage and, according to some experts, have resulted in the largest ever involuntary transfer of wealth.[142] During a 2012 congressional hearing on cyber security, Congressman Michael McCaul stated that America is under attack by "digital bombs" and publicly acknowledged a committee report that found China had stolen "several terabytes of data related to design and electronics systems of the F-35 Lightning II, one of the most

---

137 Amrita Jayakumar, "Data Breach Hits Target's Profits, but That's Only the Tip of the Iceberg," *The Washington Post*, February 26, 2014, http://www.washingtonpost.com/business/economy/data-breach-hits-targets-profits-but-thats-only-the-tip-of-the-iceberg/2014/02/26/159f6846-9d60-11e3-9ba6-800d1192d08b_story.html.

138 Ibid.

139 Wilshusen, *Cybersecurity: Threats Impacting the Nation*.

140 Ibid.

141 Ibid.

142 "Investigations Inc.: Cyber Espionage: The Chinese Threat," *CNBC*, July 3, 2012, http://www.cnbc.com/id/47962225#.

advanced fighter planes under development."[143] At a cost of over $400 billion, the F-35 Lightning II is considered to be one of America's most costly weapons program; yet, the design and production edge for this important national defense tool has been already compromised providing America's competing national powers a substantial advantage in implementing their own national defense strategies.[144]

Nations states also use cyber power as a useful strategic instrument since it can be wielded globally with a certain degree of anonymity in peace, crisis, and war.[145] When used to attack critical systems, such as national infrastructure, the use of cyber power can potentially blur the distinction between peace and war resulting in increased risk to national security.[146] These risks were demonstrated in the 2007 Estonia cyber attack. The Estonia attacks were largely attributed to patriot hackers motivated to support a Russian nationalist protest against the movement of a Soviet era memorial from Tallinn. However, the Estonian government believes these hackers acted under the direction of the Russian government serving as a buffer between the true intentions of the Russian government and the so-called autonomous hacktivist community.[147] However, the sophistication of encryption and anonymizer tools available on the web makes it increasingly difficult to attribute such actions. Governments, taking advantage of these tools, may utilize hacktivists, patriot hackers, and organized criminal groups to conceal state sponsored activity and create campaigns of disruption built upon contagion within these groups. These blurred lines of distinction highlight the danger of anonymity and activism when nation states also have a general interest in a movement's outcome. Others believe nation state activity on the web is reflective of change in the "character of war"

---

143 Christopher Goins and Pete Winn, "Chinese Hackers Stole Plans for America's New Joint Strike Fighter Plane, Says Investigations Subcommittee Chair," *CNS News*, April 25, 2012, http://cnsnews.com/news/article/chinese-hackers-stole-plans-americas-new-joint-strike-fighter-plane-says-investigations.

144 David Alexander, "Theft of F-35 Design Data Is Helping U.S. Adversaries," Reuters, June 19, 2013, http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619.

145 James J. Wirtz, Colin S. Gray, and John Baylis, *Strategy in the Contemporary World: An Introduction to Strategic Studies*, Kindle Edition (Oxford, United Kingdom: Oxford University Press, 2012), 316.

146 Ibid.

147 Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington Post*, May 19, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

and the new norm in international politics. If true, then nation state cyber activity can be perceived as "a kind of background noise to the everyday dynamics of international relations" and the beginning of the age of perpetual disruption.[148]

Such cyber activity can create serious national security concerns causing some countries to calculate their engagement in this area. Recognizing the escalation in nation state cyber activity and the problem of attribution, the U.S. and Russia agreed in 2013 to implement a nuclear hotline for communication during times of cyber crisis.[149] According to the *Washington Times*, this was done to prevent "errors in judgment or misunderstanding that could escalate into war."[150]

C. HACKTIVISM

The term hacktivism has many derivations; however, it is mostly used to describe hacking activity in support of a social movement or cause. Nadav Morag, Professor and PhD at the Naval Postgraduate School, defines a hacktivist as "an individual who uses computers and computer networks to disrupt operations and/or expose sensitive information for political or social reasons."[151] Dorothy Denning, also at NPS, describes hacktivism as the elevation of civil disobedience into cyberspace; activism meets the hacker.[152] In a sense, the term hacktivism is used to define a political movement that uses the Internet for direct action tactics to cause or influence political change. Much like the Greenpeace activists who confront whaling ships in the high seas, hacktivists confront the target of their protests on the Internet, taking advantage of the world's increased reliance on the web for daily operations.

---

148 Wirtz, Gray, and Baylis, *Strategy in the Contemporary World*, 316.

149 Shaun Waterman, "Cold War Throwback: U.S.-Russia to Use Nuclear 'Hotline' for New Cyber Showdown," *The Washington Times*, June 18, 2013, http://www.washingtontimes.com/news/2013/jun/18/cold-war-throwback-us-russia-use-nuclear-hotline-n/.

150 Ibid.

151 Nadav Morag, "Hacktivists: Cyber Freedom Fighters or Cybercriminals?," Colorado Technical University, November 22, 2013, http://www.coloradotech.edu/resources/blogs/november-2013/hls-hacktivists?form=degreetype&code=5484&utm_source=Internal&utm_medium=newleadform&utm_campaign=newleadform_no_tcpa.

152 Denning, "Activism, Hacktivism."

Others define hacktivism in less sinister tones. Peter Krapp suggests that hacktivism is a controversial term and points out that many are willing to equate hacktivists as programmers with critical thinking skills interested in expressive politics, free speech, human rights, or information ethics.[153] Denning adds to this debate and offers that some see hacktivism as "conceptual net art that empowers people through active/artistic expression."[154] Acknowledging the ambiguity surrounding its definition, Krapp also suggests, "No common goal or motivating movement allows us to understand hacktivism in its social or political context."[155] Despite these differing variables, hacktivists use basic methods similar to that of other cyber criminals to achieve their goals. As we will explore in the next chapter, hacktivists are opportunistic and have numbers on their side. However, unlike cyber criminals, hacktivists much like the nation state actors in Estonia, aim to "maximize disruption and embarrassment to their victims."[156]

Hacktivists, whose origins date back to the 1980s, have access to and utilize a number of tools and techniques to elevate awareness of a social cause. In 1987, a German hacker group called BayerischerHackPost (BHP) attempted to attack German government computer systems that stored census information "in the belief that the government should not collect personal information."[157] In 1989 and in support of protest against the launch of the U.S. Galileo satellite powered by plutonium, unknown hackers deployed a worm to deface the Department of Energy and NASA websites with an anti-nuclear message for peace.[158]

Though then appearing as little more than a nuisance, the actions of BHP and the deployment of the WANK worm reflected a change in the landscape for political

---

153 Peter Krapp, "Terror and Play, or What Was Hacktivism?" Grey Room 21: Massachusetts Institute of Technology, 2005, http://www.academia.edu/307639/Terror_and_Play_or_What_Was_Hacktivism, 73.

154 Denning, "Activism, Hacktivism, and Cyberterrorism," 27.

155 Krapp, "Terror and Play, or What Was Hacktivism?," 73.

156 Verizon, *2013 Data Breach Investigations Report*.

157 Kent Anderson, *Hacktivism and Politically Motivated Computer Crime*, Encurve LLC, 2008, http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf, 5.

158 "WANK Worm on SPAN Network," CERT, October 17, 1989, http://www.cert.org/historical/advisories/CA-1989-04.cfm.

discourse and highlighted the power of the Internet as a tool for social change. Since this attack in 1989, hacktivists have utilized a number of tactics to promote political causes, chiefly free speech, human rights, and information ethics.[159] Unfortunately, the WANK attack has not been the norm and set the stage for a significant evolution of activism on the web. In June 1998 members of the hacktivist group Milw0rm, a unique group united only by the Internet, seized control of six servers at India's Bhabha Atomic research center in Bombay and downloaded thousands of pages of email messages and research that contained analysis and discussion of India's nuclear testing and test detonations.[160] A year later in 1999, the hacktivist group Electrohippies, in support of the massive street protests against the Seattle World Trade Organization Ministerial Conference, conducted a denial of service attack against server networks that supported the meetings effectively slowing down and completely halting the conference networks.[161] The hacktivist group claimed to have effectively utilized 450,000 people to conduct their attack reflecting massive solidarity with the protest movement. The act also demonstrated an effective and significant relationship between hackers and the then nascent anti-globalization movement. The protests very effectively drew attention to the anti-globalization movement and supporting arguments. Though many consider such criminal acts a "nuisance," hacktivists believe they are acts of civil disobedience and treasured expressions of free speech to promote social change.

Hacktivism itself comprises of many sub-groups that, although linked by their desire for social or political change, are motivated by different factors. According to McAfee, hacktivism combines three major groups as follows:[162]

1. **Anonymous**, an infamous social movement component that is actively involved in hacking, DDoS, and stealing and distributing personal and/or confidential information.

---

159 Krapp, "Terror and Play, or What Was Hacktivism?," 73.

160 Kendall R. Joseph, *Global Information Systems Threats: Issues in System Security in the New Age of Hactivism, Cyberterrorism and Cyberwarfare* (Murfreesboro, TN: Middle Tennessee State University, 2003), http://www.zachevans.org/wp-content/uploads/2012/02/Global_Information_Systems_Threats.pdf.

161 Tim Jordan and Paul Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (New York, New York; Taylor & Francis, 2004), 75.

162 Paget, *Cybercrime and Hacktivism*, 3.

2. **Cyber dissidents**, considered by McAfee to be "the real activists" who primarily use the Internet and social networks for coordination to spread propaganda and information. They attempt high high-profile actions on the Internet in hopes of bolstering democracy and fighting corruption in their countries.

3. **Cyber warriors** are described as patriotic hackers who "claim to act on behalf of their governments by supporting national and extremist movements."[163] Numerous politically charged skirmishes and government actions throughout the world provide motivation for turning hackers into hacktivists.

Although not mentioned in the McAfee report, a real-world component also exists to compliment the hacktivist effort. Websites, such as WikiLeaks and the now defunct Exposed.su, have been set up to provide secure and anonymous ways for sources to leak personal information and sensitive documents for global public consumption.[164] Although not personally involved in the hack, such sites offer real opportunity for hacktivists to expose their targets reaching millions of people in the process.

Anonymous and likeminded hacktivist groups will be further discussed in subsequent chapters; however, its avenging role against commercial, private and government sector entities has greatly increased forcing Verizon to declare 2011 as the year of the hacktivist. In 2011, despite accounting for only three percent of the data breach activity, hacktivists, and in particular Anonymous and its subgroups, accounted for the theft of an astonishing 100 million of the 177 million individual records stolen throughout the year.[165] These statistics do not include the normal hacktivist activity, such as DDoS and website defacement, but rather, a graduating tactic with significant consequence. In 2011, Anonymous and its sub-group LulzSec targeted Sony to avenge what the group declared an "unforgivable offence against free speech and Internet freedom."[166] In response to Sony's efforts to seek prosecution against a hacker who circumnavigated the security systems of Sony PlayStation 3, Anonymous and affiliated

---

163 Ibid., 3.

164 "About: What Is Wikileaks?," *WikiLeaks*, May 7, 2011, https://wikileaks.org/About.html.

165 Verizon, *2012 Data Breach Investigations Report*, 20.

166 Sara Yin, "'Anonymou' Attacks Sony in Support of PS3 Hackers," *PCMag*, April 4, 2011, http://www.pcmag.com/article2/0,2817,2383018,00.asp.

hackers targeted Sony's online gaming servers compromising 12 million financial account records for Sony's online user community.[167] Sony suffered total revenue loss of approximately $123 million as a result of the intrusion.[168] This hack also revealed the indiscriminate nature of hacktivist attacks and also the potential for splinter groups within organizations such as Anonymous. The Anonymous sub-group LulzSec, largely believed to be behind the Sony attack, also went on an anti-government campaign that targeted a number of government websites and the sensitive data on its servers. The aggressive nature of their actions is potentially indicative of the willingness of a smaller sub-group to act out in undisciplined ways on the web.

Although the nature of the cyber threat may vary, cyber threat actors utilize similar tactics and methods to accomplish their goals. Advanced persistent threats such as nation state cyber activity reflect the most sophisticated and perpetual cyber threats; however, the life cycle for criminal and hacktivist threats appears to be limited only by motivation and not their skillset; the previously noted availability of malware, toolkits and underground networks supports this.

D. CONCLUSION

However, what the methods do not imply is their motives. In order to understand the potential increased risk posed by hacktivists, it is necessary to further explore the actions of Anonymous and its subgroups compared to similarly motivated terrestrial based groups. If Anonymous and likeminded hacktivist groups are truly motivated by social dynamics and ideology, it is possible that continued evolution of such movements would entail use of increasingly disruptive cyber based tactics. As previously discussed, such cyber-based threats are real, accessible and capable of causing physical harm to U.S. infrastructure. This level of disruption, though not yet realized in the U.S., can have significant cascading effects that may potentially include harm or death to persons. The

---

[167] Keith Stuart, "Why Are Lulzsec and Anonymous Hacking Games Companies?," *The Guardian*, June 16, 2011, http://www.theguardian.com/technology/2011/jun/16/lulzsec-anonymous-hacking-games-companies.

[168] Robert Vamosi, "How Hacktivism Affects Us All," PCWorld, September 6, 2011, http://www.pcworld.com/article/239594/how_hacktivism_affects_us_all.html.

previous two chapters have revealed the difficulty in not only identifying cyber based threat actors but in also containing the effects of their actions. Unlike a bomb or bullet that finds its target, cyber weapons have long lasting presence on the web with immediate accessibility.

THIS PAGE LEFT INTENTIONALLY LEFT BLANK

IV. RISKY SHIFT

The individual threat posed by cyber threat actors is genuine as evidenced by the relative ease with which lone subjects can obtain and use cyber based tools and weapons. However, in attempting to further understand the potential threat posed by hacktivism, consideration must also be given to the Internet's ability to serve as an enabler for social movements to splinter into more radical factions. In the 1960s and 1970s, the university campus served as a platform for communication and quick assembly resulting in a number of civil rights and anti-war movements around the United States. Campus sit-ins and clashes with authority distinguished their movement and memorialized their cause; however, more radical members employed terrorist tactics and formed direct action groups. This is evidenced by the social movement called the Students for a Democratic Society, who after repeated confrontations with authority, failed to galvanize its members beyond its broad based agenda. The resulting discourse forced more radical members to splinter and create a violent group known as the Weather Underground. Such discourse is not unusual for terrestrial-based movements as evidenced by the number of social movements and terrorist groups around the world. However, the recent explosion of social media and other web-based communication platforms offers a unique opportunity for social movements and discourse to evolve online. This chapter will further explore the ideological and cognitive effects that the Internet and social media has on the congruence of hacktivists and social discourse by examining the social science of collective behavior and its effects on cohesion, discourse, and fracture. Additionally, since the Internet provides the technical advantage of concealment, the effects of anonymity on individual and collective behavior will be further examined to further comprehend the possible impact of hacktivism.

A. COMMUNICATIVE AND COLLECTIVE IMPACT OF SOCIAL MEDIA

The emergence of social media and message boards on the Internet has resulted in increased communication, networking, and increasing reliance on digital infrastructure that can "empower transnational resistance movements and create new vulnerabilities for

nation-states."[169] Social media and other mass communication platforms enable quick congruence on hot topic issues creating a shared identity for once thought to be innocuous issues. This shared identity, as realized in Estonia and in the support of the revolutionaries of the Arab Spring, "demonstrated an international solidarity that structured itself without any hierarchy" and reveals the power of digital technology and its ability to rapidly mobilize groups of people in times of crisis.[170] As noted by Jornod Rodhlann and as seen in the Industrial Revolution, "technological progress has stimulated societal transformations and whipped up revolutionary sentiment."[171]

When one considers the growth of social media and inherent ability for increased situational awareness, it is difficult to argue against the impact of this technology. Eliminating the challenge of time and space, social media connects people from all over the world together, creating increased opportunities for political awareness and organization. The Ukrainian Orange Revolution in 2004 is a real example of the impact of this technology. Citizens of Ukraine, upset with the results of a presidential election largely marred by the corrupt tactics of intimidation by the incumbent's regime, conducted a series of protest actions that included acts of civil disobedience and general strikes. Taking advantage of the structural weakness within the incumbent regime, protesters circumvented authoritative efforts to squash their protest through effective use of the Internet and its web based communication tools.[172] Citizen journalists offered their dissenting opinions on web-based message boards circumventing the government's self-censored media environment. Protesters also used mobile phones and the Internet to coordinate a wide range of activities, including election monitoring and wide-scale protests. With growing national unrest and increasing international attention, the incumbent leader was forced to hold a runoff election resulting in the regime's demise

169 Herzog, "Revisiting the Estonian Cyber Attacks."

170 Jornod Rodhlann, "Hacktivism: The Road to Anarchism?" MyScienceWork, January 22, 2014, https://www.mysciencework.com/news/11093/hacktivism-the-road-to-anarchism.

171 Ibid.

172 Joshua Goldstein, *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution* (Cambridge, MA: Harvard Law School, Berkman Center for Internet & Society, 2007).

and a victory for the opposition and the Ukrainian protestors.[173] In his paper regarding the role of digital technology in the revolution, Joshua Goldstein states, "the Orange Revolution would not have happened without the Internet"[174]

Today, supported in part by over one billion registered smart cell phones, the Internet is accessible to almost anyone with electricity and the access to the web.[175] At the end of 2013, the number of active worldwide social media users totaled approximately 1.73 billion equating to one quarter of the world's population.[176] During the five-year period leading up to 2013, social media was credited for the "first social media President," the Arab Spring and the Occupy Wall Street movement.[177] Social media enables millions of people to communicate at a moments notice, not only increasing political awareness, but also providing an organizing platform for activism. According to a 2009 digital activism survey, the "prominence of social networks as the 'gateway drug' of digital activism is noteworthy" and was noted as the most common "first tool" for activists.[178] This is unsurprising since the accessibility of the web and its Internet based tools are user friendly and, as previously noted, incredibly adept at formulating direct action.

However, despite this "gateway," some believe that activism, and in particular student activism is indolent. During the height of the Occupy Movement in 2011, a survey of professors at Brown University revealed that a majority of the faculty members believed that student activism is lower today than when they themselves attended college.[179] According to the survey, of the faculty who have worked at Brown for more

---

173 Adrain Karatnycky, "Ukraine's Orange Revolution," *Foreign Affairs*, April 2005, http://www.foreignaffairs.com/articles/60620/adrian-karatnycky/ukraines-orange-revolution.

174 Goldstein, *The Role of Digital Networked Technologies*, 19.

175 Don Reisinger, "Worldwide Smartphone User Base Hits 1 Billion," CNET, October 17, 2012, http://www.cnet.com/news/worldwide-smartphone-user-base-hits-1-billion/.

176 Evan LePage, "The Evolution of Social Media," Social Media Today, December 1, 2013, http://www.socialmediatoday.com/content/evolution-social-media-infographic.

177 Ibid.

178 Katherine Brodock, Mary Joyce, and Timo Zaeck, *R@D 4—Digital Activism Survey Report 2009*, July 14, 2009, http://www.slideshare.net/DigiActive/rd-4-digital-activism-survey-report-2009.

179 Neelkiran Yalamarthy, "Profs See Waning Student Activism," *Brown Daily Herald*, October 25, 2011, http://www.browndailyherald.com/2011/10/25/profs-see-waning-student-activism/.

than 20 years, 82.6 percent reported student activism is lower or much lower.[180] The survey reveals an interesting perspective on activism and supporting social movements. The social movements of the 1960s and 1970s occupied physical space and were tangible for professors and authority alike. Racial segregation, the Vietnam War, and women's rights issues helped to fuel nationwide campus protests. A galvanized student population solidified the existence of the Students for a Democratic Society as the leading student group against the war in Vietnam. Campus sit-ins and clashes with authority distinguished their movement and memorialized their cause, however, more radical members employed terrorist tactics and formed direct action groups like the Weather Underground and Earth Liberation Front. It would seem then, that the opaque agenda of the Occupy Movement, though effective at drawing attention to globalization theory, at least from the viewpoint of the Brown professors, was not unifying and void of the flashpoints associated with previous student movements.

Lauren Schleimer, columnist for the Brown Daily Herald, disagrees stating, "students just don't protest like they used to."[181] Reinforcing the Internet's role in activism, Schleimer notes that the Internet and social media have made it easier to organize a popular uprising and points to the Arab Spring as an example.[182] In December 2010, a Facebook video of a Tunisian fruit vendor setting himself ablaze to protest the corrupt tactics of the Tunisian government served as the tipping point for a series of rebellious protests by Tunisians exasperated by years of high unemployment and limited personal and political freedoms.[183] The actions of the protesters also galvanized the support of hacktivists around the globe, who showing solidarity with the movement, disabled several Tunisian government sites and provided Tunisian protestors with tools to

---

180 Ibid.

181 Lauren Schleimer, "Schleimer '12: What Happened to Student Activism?," *Brown Daily Herald*, March 8, 2012, http://www.browndailyherald.com/2012/03/08/schleimer-12-what-happened-to-student-activism/.

182 Ibid.

183 "Arab Spring," Global Issues in Context, 2014, http://find.galegroup.com/gic/infomark.do?docType=GREF&prodId=GIC&type=retrieve&version=1.0&idigest=b527955b5caccdb4b4a2d40e86fe061a&userGroupName=cant48040&docId=CP3208520388&contentSet=GREF&source=gale.

avoid government detection on the Internet.[184] Hacktivists redeployed dialup modem pools to establish communication channels to aid and guide protest movements strengthening the protestors' resilience against government forces.[185]

The lens used to view activism can affect how one views the impact of a social movement. The university professor reflects upon galvanizing issues of the 1960s and recounts how such movements shaped discourse in America. Others argue that activism is alive and well and has actually moved beyond terrestrial into cyber.[186] Tunisia and the Orange Revolution are real examples of how hacktivists, taking advantage of public sentiment and structural vulnerabilities within a government, can leverage the power of the Internet to strengthen movements. Though only a small part of the overall movement, hacktivists have effectively displayed their ability and willingness to engage in powerful protest actions. It would then appear that digital activism is lesser understood for its impact and is misunderstood in the context of larger movements. Activists today freely exchange ideas in open forums gaining access to millions of people in the process. By connecting individuals to broad social movements, social media brings individual micro thought to a macro level where it can be harnessed by the masses. Occasionally, from these debates emerge movements, such as Occupy and the Arab Spring, two movements considered significant for its social impact and ability to garner mass media attention. By sustaining discrete communication platforms for use by Middle East protestors, hacktivists played a small part in sustaining protest efforts. It is in this context that the power of the Internet and hacktivism may be greatly underestimated.

B. STRUCTURE

The strength of a group is determined by its organizational structure.[187] Social movements traditionally have had many organizationally distinct components that

---

184 Marc Fisher, "In Tunisia, Act of One Fruit Vendor Sparks Wave of Revolution through Arab World," *The Washington Post*, March 26, 2011, http://www.washingtonpost.com/world/in-tunisia-act-of-one-fruit-vendor-sparks-wave-of-revolution-through-arab-world/2011/03/16/AFjfsueB_story.html.

185 "Hacktivism, Tools, and the Arab Spring," HN9A06, *2600—The Hacker Quarterly*, July 13, 2012, http://store.2600.com/hatoandarsp.html

186 Schleimer, "Schleimer '12: What Happened to Student Activism?"

187 "Terrorist Groups," accessed September 8, 2014, http://www.terrorism-research.com/groups/.

"change through fission, fusion and new creation."[188] These components are sometimes purposeful for command and control and others a result of splinters or defined roles and responsibilities, such as those within cyber-criminal organizations. Larger collectives like the SDS, a student body movement, also had many campus chapters influenced by various ideologies and beliefs resulting in subgroups of Marxist, Socialist, Maoist, and worker's rights alliances within the larger anti-Vietnam War collective. As an Internet-based collective, hacktivists rely on collective action for target selection and action since most members are joined virtually via the web from around the globe. In these movements organizational structures and processes are an "action form" or "method of protest in itself" rather than a means for resource mobilization.[189] Thus, the action is the cause that sets the movement in motion.

What motivates the action, especially in reform movements, is what also defines its structure. Since the 1960s, social movements in America have attempted to work within the established order and preserve some existing values, such as equal opportunity, preservation of the environment, or as is the case with most hacktivists, freedom of speech. The Civil Rights Movement of the 1960s was not subversive but rather worked to change socio-economic conditions within the existing social and governmental frameworks. In order to achieve such goals, movements require the development of at least ephemeral organizational structure to overcome the challenges of resource mobilization and funding. However, hierarchy and structure are often the qualities of government that social movements are trying to change thus are "counterproductive to the group's ideals."[190] In his thesis, about the evolution of Anonymous, Max Halupka states that the restriction of hierarchical structure causes political movements to

---

188 Luther P. Gerlach, "The Structure of Social Components: Environmental Activism and Its Opponents," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and John Rondfelt (Santa Monica, California: RAND, 2001), 290.

189 Abigail A. Fuller, *The Structure and Process of Peace Movement Organizations: Effects on Participation* (Boulder, CO: University of Colorado, 1989).

190 Rudolf Heberle and Joseph Gusfield, "Social Movements Facts, Information, Pictures," *Encyclopedia*, 1968, http://www.encyclopedia.com/topic/Social_movements.aspx.

disengage and seek alternative forms of governance.[191] The result is often a leaderless decentralized network that effectively embraces the collective.

Decentralized networks consist mainly of nodes or cells that although part of a larger collective, are usually not beholden to any single point of control. The ideology or purpose determines its actions. Each node possesses a certain amount of autonomy; however, is expected to act in accordance with the group's goals. Alignment with the group's goals is achieved through communication platforms, such as publications, journals or, as in the case of hacktivism, web-based communication platforms. Discourse between nodes or with the larger network can lead to schism resulting in one or more nodes either dissolving or splintering to form a separate group.

A secondary characteristic of decentralized networks in virtual environments is the ability for these networks to swarm around a particular issue or cause. Swarms are informal partnerships that are created spontaneously by people who share common interest or ideologies without leadership.[192] Collaboration is a byproduct of the swarm and not the cause of it. However, swarms are always collaborative as members are motivated by being part of the larger group. As a virtual entity, "trust is assessed via reputation in online illicit activities."[193] Anonymous, as a reactive body, is reflective of a swarm group that, as a result of web based communication platforms, is highly responsive to emerging issues. (See Figure 1).

---

191 Halupka, "The Evolution of Anonymous as a Political Actor," 25.

192 Roderic Broadhurst et al., "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime," *International Journal of Cyber Criminology* 8, no. 1 (2014), http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf, 5.

193 Ibid.

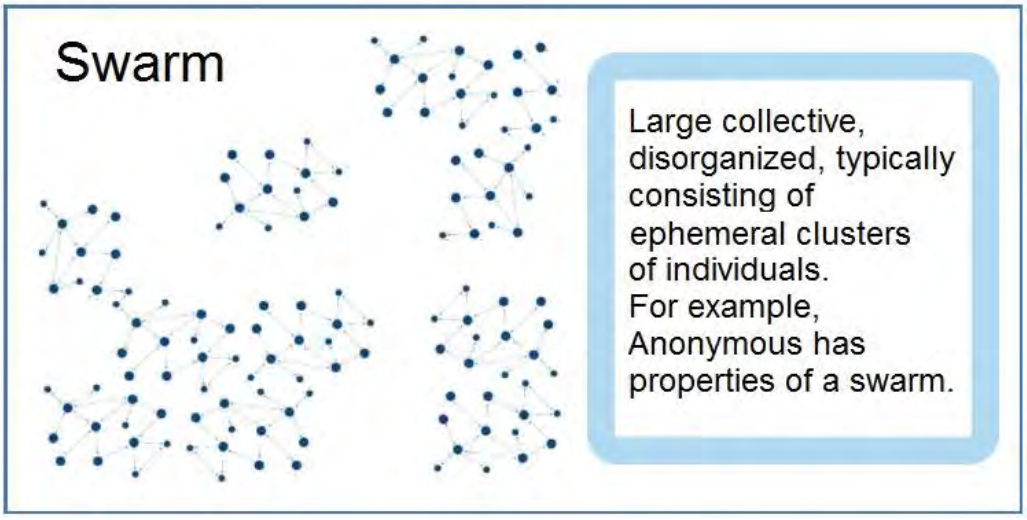

Figure 1. Model of Swarm Style of Convergence[194]

Activists favor decentralized networks because its structure makes "insurgency and infiltration difficult" allowing even more extreme elements to remain resilient against authoritative action.[195] Radical environmentalist movements utilize decentralized networks to effectively implement tactics of direct action. Likewise for the SDS, who after attempting to use a structured environment, fell into a more linear network of campus chapters, each with individual leaders galvanized behind an anti-capitalist agenda. As will be discussed in subsequent chapters, hacktivists, in particular the group Anonymous, utilize decentralized networks to perform target selection and direct action via web based communication platforms.

C. FRAMING THE DISCOURSE

Activist use of the Internet to communicate and organize is greatly enhanced by the web's "distributed architecture and its scale-free topology."[196] Social media provides a unifying framework for the emergence of cooperation and formation of scale free networks. Community blogs like Facebook were unwittingly designed to enable collective action. Likeminded individuals are drawn to similar interests on the web

194 Ibid.

195 Halupka, "The Evolution of Anonymous as a Political Actor," 26.

196 Joss Hands, *@ Is for Activism* (London, United Kingdom: Pluto Press, 2011).

through hubs like Facebook and Twitter creating additional dialogue and smaller communities on the web. Joss Hands, author of the book *@ is for Activism*, refers to these "bonds of recognition" as impacting not only what people may agree about but also their differences.[197] According to Hands, when we put "distributed networks together, opportunities to engage in dialogue, to come to agreement and act necessarily scale up."[198] The Internet exponentially increases the likelihood of finding likeminded partners thus provides a distinct advantage over terrestrial based movements.

In addition to convergence, social media also provides a unique platform for individuals to frame the debate. This framing process, first coined by Erving Goffman in 1974, highlights the evolutionary manner where communicators, over a period of discussion and debate, construct a point of view that others embrace for a particular situation.[199] The result is a central organizing idea that galvanizes larger numbers via social media platforms.

Framing is often applied to social movements and is helpful to describe the effects social media has in framing hacktivist movements, such as Anonymous.[200] Felix Tusa, author of the article "Identity in Flux: Social Media and Social Movements," attests that the Internet and social media have "reinvented the process of framing," adding the Internet is a perfect tool to give context and meaning to occurrences.[201] Much like the major news networks, social media offers the ability for protestors to share information, video, and photos about an issue enabling the individual and larger group to frame an issue over time. Incorporating this power, Anonymous, showing solidarity with a Canadian-based activist magazine's call to "occupy Wall Street," posted a YouTube

---

197 Ibid.

198 Ibid.

199 Erving Goffman, *Frame Analysis: An Essay on the Organization of Experience* (Boston, MA: Northeastern University Press, 1986), http://is.muni.cz/el/1423/podzim2013/SOC571E/um/E.Goffman-FrameAnalysis.pdf.

200 David A. Snow and Robert D. Benford, "Ideology, Frame Resonance, and Participant Mobilization," in *From Structure to Action: Social Movement Participation across Cultures*, ed. Bert Klandermans, Hanspeter Kriesi, and Sidney Tarrow, 197–217 (Greenwich, CT: JAI Press, 1988).

201 Felix Tusa, "How Social Media Can Shape a Protest Movement: The Cases of Egypt in 2011 and Iran in 2009," *Arab, Media & Society*, no. 17 (2013), http://www.arabmediasociety.com/?article=816.

video in August 2011 drawing attention to the little known article.[202] The video announced plans to mobilize 20,000 people to lower Manhattan, which resulted in massive national media attention and security alerts from the Department of Homeland Security (DHS).[203] The end result was a multi-month assembly of over 700 people in lower Manhattan that drew intense media attention to the group's cause of social inequality. Hacktivist DDoS efforts to disrupt Wall Street operations were mostly ineffective; however, their involvement and support effectively focused global attention on the cause of social inequality. The Occupy Wall Street movement was greatly enhanced by the use of social media tools enabling a few protestors to galvanize massive virtual support for their cause.[204] The popular social media site Facebook has since become a recruiting tool for new supporters and event coordination.[205]

The recent emergences of web-based technologies have converged to provide a unique backdrop for social movements and, unlike the inherent difficulties in sustaining terrestrial movements, enhances resiliency for amorphous movements. Williams suggests that the Internet has replaced the traditional need for money and labor and is equally as important as "legitimacy, manpower, and technical expertise" in emulating the social movements of the 1960s.[206]

Much like terrestrial social movements, online activist communities also disagree resulting in the creation of smaller autonomous hubs or clusters that are less controlled by the larger majority. Hacktivists occupy this small cluster environment. Alexandra Samuel asserts that the hacktivist hub or collective actually represents a new social movement

---

202 Sean Captain, "The Real Role of Anonymous in Occupy Wall Street," Fast Company, October 18, 2011, http://www.fastcompany.com/1788397/real-role-anonymous-occupy-wall-street.

203 Ibid.

204 Andrew Fleming, "Adbusters Sparks Wall Street Protest," *Vancouver Courier*, September 27, 2011, http://www.vancourier.com/news/adbusters-sparks-wall-street-protest-1.374299.

205 Neal Caren and Sarah Gaby, "Occupy Online: Facebook and the Spread of Occupy Wall Street," October 24, 2011, http://ssrn.com/abstract=1943168.

206 Apryl Williams, "Identity in Flux: Social Media and Social Movements," The Ripple Effect, July 9, 2013, http://harmony-institute.org/therippleeffect/2013/07/09/identity-in-flux-social-media-and-social-movements/.

within the aforementioned larger collective.[207] According to Samuel, hacktivists represents an "unconventional collective behavior" with their own common discourse.[208] Thus, as actors in the in the larger collective, the hacktivist framing process can focus direction and action to resolve collective action dilemmas by "technically enabling new one person forms of action."[209] This is an important distinction as it not only denotes a stronger appreciation of the role and threat posed by hacktivists but also the autonomous nature of their decision making process.

Gladwell strengthens this argument and suggests, when it comes to online activism, decisions made by consensus very rarely create strong ties or bonds for effective change.[210] Although this structure creates group resilience in low-risk situations, change is rarely a by-product of low-risk movements. Hacktivism, as a direct action equivalent, represent a necessary risk-reward equivalent for social movements. Apryl Williams, Graduate Assistant at the Sociology Department of Texas A&M, suggests that although collective identity serves as a counterpart to individual identity management, "the sentiments that are projected on social media don't always translate to meaningful action."[211] This argument supports the opinion of the professors at Brown University and questions the limits of hacktivism and the factors and channels of protest that are required for meaningful action. The anti-war movement of the 1960s comprised of many individuals easily identifiable by authority yet the movement persisted and evolved into direct action, as evidenced by the Weather Underground. In their book *Poor People's Movements*, Piven and Cloward contend that change results from chaos and disruption and famously proposed overloading the American welfare system to force a

---

[207] Alexandra Samuel, *Decoding Hacktivism: Purpose, Method, and Identity in a New Social Movement* (Cambridge: Harvard University, 2001), http://www.alexandrasamuel.com/netpolitics/decodinghacktivism.pdf.

[208] Ibid., 4.

[209] Ibid., 5.

[210] Malcolm Gladwell, "Small Change," *The New Yorker*, October 4, 2010, http://www.newyorker.com/magazine/2010/10/04/small-change-3?currentPage=all.

[211] Williams, "Identity in Flux: Social Media and Social Movements."

new system that would guarantee equal income for Americans.[212] The effectiveness of this strategy and the use of disruption continues to be challenged by many social scientists who argue that disruption inhibits success as evidenced by the violent strikes held by labor unions in the 1900s.[213] Though challenged, the Piven-Cloward strategy of disruption remains a viable tactic in social movement and terrorist methodology.

As previously noted, groups formed by weak ties are less likely to achieve change against formative structures such as governments. However, the process of group polarization suggests that groups tend to make more extreme decisions through a process of de-individuation, or loss of individual self-awareness. The remaining group is less cautious and more likely to engage in risky behavior, a process also termed as risky shift.[214] This shift is significant since, as previously noted, the Internet provides a real platform for disruption. Hacktivist groups such as Anonymous engage in disruptive behavior in furtherance of a social cause and appear to be an online equivalent for risky shift. Anonymous represents a more extreme option for lesser capable or committed members, in this case, an online collective.

Hacktivists then are a cognitive layer within the larger discourse. As an amorphous blob, decisions are made across a single parallel and not subjected to hierarchy or hegemonic authority. This is purposeful as transgressors "seek ways to free human individuality from the bonds of representation that would contain it."[215] For example, the SDS failed to coalesce a lasting movement beyond the campus; thus, the Weather Underground used transgressive performances in the service of hegemonic discipline.[216] Hacktivists attempt to move social movements beyond the rhetoric towards

---

212 Frances Fox Piven and Richard Cloward, "The Weight of the Poor: A Strategy to End Poverty," The Nation, accessed March 31, 2014, http://www.thenation.com/article/weight-poor-strategy-end-poverty.

213 Philip Taft and Philip Ross, "American Labor Violence: Its Causes, Character, and Outcome," in *The History of Violence in America: A Report to the National Commission on the Causes and Prevention of Violence*, ed. Hugh Davis Graham and Ted Robert Gurr, 1969, http://www.ditext.com/taft/violence.html.

214 Conrad Anker, *The Risky Shift Phenomenon: What Is It, Why Does It Occur and What Are the Implications for Outdoor Recreationists?*, Central Washington, University, http://www.geology.cwu.edu/dept/courses/g410/handouts/risky_shift.pdf.

215 Foust, *Transgression as a Mode of Resistance*, 209.

216 Ibid., 210–211.

action and recognize that the representative debate process "dilutes the potential effects of concrete action" necessitating a distinct and separate hacktivist cluster or movement.[217] Samuel highlights this inevitable outcome and describes hacktivist groups as a "self-defined, discursive, unconventional collective action movement."[218] They are mostly void of purpose but rather a method looking for a cause akin to a bomb maker in search of a terror group. Their technical capability distinguishes them as a means based movement in search for "specific purposes or political issues that can serve as targets for their hacktivist practices."[219]

The lack of hierarchy or control in decentralized networks such as Anonymous, although, beneficial to resiliency and communication, also opens the network to a larger collection of ideas, which, as discussed, leads to discourse and tension. Thus, the conditions that create decentralized movements are sometimes subject to debate and, although not harmful to the majority, may isolate cells and/or clusters within the group.

In general, most social movements focused on policy or institutional change embrace "polite" protest tactics "aimed more at attracting media attention and influencing public opinion than using disruption as a tactic of last resort."[220] However, according to Hank Johnston, author of the book *States and Social Movements,* although highly organized, these less effective tactics tend to isolate those cells or clusters holding more extreme ideological stances.[221] Radical members of the environmental group Earth First!, frustrated with the group's unwillingness to escalate its use of direct action, splintered to form a more extreme group called the Earth Liberation Front that, remaining aligned with the cause of environmentalism, utilized more damaging tactics of arson and property destruction. Johnston notes that the failure to sustain even the extreme movement results in some members becoming more isolated and, unwilling to compromise.[222] This results

---

217 Ibid.

218 Samuel, *Decoding Hacktivism: Purpose, Method, and Identity in a New Social Movement*, 5.

219 Ibid., 6.

220 Hank Johnston, *States and Social Movements* (Cambridge, United Kingdom: Polity Press, 2011).

221 Ibid.

222 Ibid.

in the creation of persistent fringe elements within moderate groups. Considerable risk can emerge when the radical group persists and obtains a sense of legitimacy from more reasonable moderate members.

In addition to ideological differences, groups can experience fracture when members or cells take initiative to further the cause sensing personal power as a result of their skill and/or abilities. A 2005 letter from al-Qaida leader Ayman al-Zawahiri criticized then leader of al-Qaida's network in Iraq Abu Musab al-Zarqawi for his abhorrent tactics of hostage beheadings and increased conflict with Shi'a Muslims rather than remain focused on al-Qaida's strategy of engagement with the U.S. military.[223] The letter revealed that al-Zarqawi acted independently and did not accept direction from al-Qaida leadership; however, the success of al-Zarqawi's network in Iraq forced an uneasy alliance with al-Qaida leadership who could no longer deny his influence and following.[224] Al-Zarqawi felt it necessary to take initiative in achieving the movement's goal in Iraq thus did not seek or wait for permission.

According to Luther Gerlach, most division occurs during the growth phase of a movement and contributes to its expansion.[225] Decentralized groups make decisions through consensus; however, as previously noted, these decisions can also be influenced by stronger personalities. The division that results tends to create new radical groups that are more likely to reject authority and organization.

D. ANONYMITY

One of the more forceful and concerning consequences of collective behavior is the dominating effects that the collective can have on individual behavior. According to social psychologists, individuals, when acting within a group setting, are susceptible to deindividuation or a loss of self-awareness. According to Jenna Chang of Baylor University, deindividuation theory asserts that the effect anonymity has on producing

---

223 David Ensor, "Al Qaeda Letter Called 'Chilling,'" *CNN*, October 12, 2005, http://www.cnn.com/2005/WORLD/meast/10/11/alqaeda.letter/.

224 Lee Hudson Teslik, "Profile: Abu Musab Al-Zarqawi," Council on Foreign Relations, June 8, 2006, http://www.cfr.org/iraq/profile-abu-musab-al-zarqawi/p9866.

225 Gerlach, "The Structure of Social Components."

uninhibited behavior is dependent upon group size; "the larger the size of the group, the higher the degree of anonymity experienced by the group's members."[226] This immediately highlights the risks associated to online collectives since social media provides a unique platform for larges masses to gather anonymously. The previously discussed influence of groupthink combined with the risks associated to anonymity make online collective more susceptible to antisocial behavior. As cited by Chang, when using the Internet, people who used computer mediated communication and whose identities were unknown showed a greater tendency to exchange "flaming behavior," such as hostile and threatening messages etc.[227] The i-SAFE foundation, a non-profit Internet safety organization, supports this claim as statistics revealed that "over half of adolescents and teens have been bullied online" with more than one in three young people have experienced cyber threats online.[228]

Distinguished psychologist Philip Zimbardo submits that when acting in an anonymity-conferring environment, a person will increase aggression such that he will feel the pleasure in destruction, vandalism and, the power of being in control.[229] Anonymity also effectively diminishes concern for self-evaluation resulting in personal disregard for following societal norms of behavior.[230] Thus, behind the mask, people are more likely to regress and when influenced by others in similar circumstances and engage in more risky or aggressive behavior. This social phenomenon is not unique or isolated to a particular venue or setting but rather inherent in the social construct of the individual mind. As a collective born of the Internet, hacktivists have already gained the distinct advantage of anonymity as evidenced by previously described anonymizer tools, such as Tor; the effects of collective behavior serves to exacerbate the risk of aggression.

---

226 Jenna Chang, "The Role of Anonymity in Deindividuated Behavior: A Comparison of Deindividuation Theory and the Social Identity Model of Deindividuation Effects (SIDE)," *The Pulse* 6, no. 1 (2008), http://www.baylor.edu/content/services/document.php?id=77099, 2.

227 Ibid., 3.

228 "Cyber Bullying Statistics," Bullying Statistics, 2013, http://www.bullyingstatistics.org/content/cyber-bullying-statistics.html.

229 Melissa Dittman, "What Makes Good People Do Bad Things?," *Monitor* 35, no. 9 (2004), http://www.apa.org/monitor/oct04/goodbad.aspx, 68.

230 Chang, "The Role of Anonymity in Deindividuated Behavior."

In another study, group interactions between people who believed they were communicating anonymously were six times more likely to make uninhibited remarks than those who believed they could be identified.[231] As social media enables more people to participate in discussion, the anonymity of these platforms undoubtedly increases the level of discourse. However, the global nature of social media and the Internet entails that web-based discussions are marked by the distance between the participants. According to Wallace, it is easier to attack someone if they are out of sight and far away as it removes the expression of fear or anguish while simultaneously providing safety and immunity from reprisal.[232]

Anonymity also offers the positive benefit of self-disclosure, a desirable feature present in many support groups, such as Alcoholics Anonymous. A treasured commodity for discourse in the political process, anonymity protects participation in the political process as evidenced by the democratic voting processes.[233] websites like change.org enable users to digitally sign petitions for organizations and causes they are passionate about. Confidential participation allows users to freely express their personally held beliefs without fear of reprisal, embarrassment, or shame.[234] People are free to speak their conscious.[235]

However, the impact of anonymity on behavior is arguably supplanted by the tactical advantage it provides to the adversary. According to Lieutenant Colonel (Lt. Col.) Iverson, anonymity affects the strategies of denial and deterrence because both assume that the potential opponent and his capabilities are known.[236] The proliferation of technology such as weaponized malware exacerbates the issue since hacktivists gain both

---

231 Patricia Wallace, *The Psychology of the Internet* (Cambridge, United Kingdom: Cambridge University Press, 2001), 125.

232 Ibid., 126.

233 Ibid., 240.

234 "Business Model," Change.org, accessed August 20, 2014, http://www.change.org/about/business-model

235 Samuel, "Hacktivism and the Future of Political Participation," 214.

236 David R. Iverson, *The Ring of Gyges: Anonymity and Technological Advance's Effect on the Deterrence of Non-State Actors in 2035* (Montgomery, AL: Air War College, 2011), http://www.au.af.mil/au/awc/awcgate/awc/2011_iverson.pdf, 2.

the capability for disruption without the possibility of detection. This is concerning since the motivation for attack increases with the decreasing ability for detection; "Instead of a rich vs. poor discriminator, technology may make an individual's anonymity a determining factor in his calculus to carry out an attack."[237]

Samuel states that hacktivists use anonymity as shelter from legal consequences such that it gives them the freedom to "mock perceived hegemonies and to release 'incorrect' but genuine feelings."[238] Thus, the choice of anonymity and accountability is a matter of "risk tolerance;" the hacktivist engaged in illegal actions will take great measures to conceal his/her identity, while lesser skilled or gullible hacktivists will accept a degree of risk because of their greater trust in the network. This is evidenced by the safety in numbers offered by the size and scope of the Anonymous collective.

E. CONCLUSION

Understanding how discourse is transformed into action is critical when attempting to understand the impact of structure and technology on activism. It is apparent that the communicative advantages of the web have eliminated the need for money and resource, which enables social movement to quickly evolve online. However, the decentralized architecture of the Internet has also introduced scores of people to decentralized networks that utilize discourse and the web for action. The structure of such groupings effects the actions of its members sometimes to the detriment of the collective cause. The additive effect of anonymity creates a risky shift that, at times, impacts the direction and action of a group. The deteriorating effect of this behavior in a leaderless network results in aggressive action that when challenged, increases friction between members. Thus, the tangible benefit of situational awareness and discourse that social media provides to the global collective ironically offers complexity behavior issues for web-based activism. More radical members are forced to consider the issue of whether the idealized individual ideas or projections offered by the majority actually contribute to

237 Ibid., 12.

238 Samuel, "Hacktivism and the Future of Political Participation," 218.

collective solutions to social issues?[239] The potential result is the existence of more cells or clusters within the group that, depending upon the conviction or level of influence of its members, may occupy more or less isolated positions within the overall network.[240] This overlapping introduces a number of changes to the network that overtime can evolve into more radical clusters of likeminded people offering skilled hacktivists with necessary conviction the perfect environment for disruption. If, as Gladwell suggests, change is a by-product of high-risk, then hacktivists may be the one component of a social movement that can achieve such ends.

Such grass roots movements exists both virtually and in the physical world and will be further studied to understand the impact of collectivist forms of organizations and the disruptive potential for web-based activists. The following three chapters will include the case studies of the Students for a Democratic Society in America, Earth First!, and Anonymous. All three movements emerged from linear or decentralized networks that formed collectivist forms of organization. Strong internal organizations emerged that when challenged, resulted in splinter formations.

239 Williams, "Identity in Flux: Social Media and Social Movements."

240 Gerben Bruinsma and Wim Bernasco, "Criminal Groups and Transnational Illegal Markets," *Crime, Law and Social Change* 41, no. 1 (February 2004): 82.

V. STUDENTS FOR A DEMOCRATIC SOCIETY

This chapter will detail the evolution of the 1960s social movement Students for a Democratic Society (SDS) and the discourse surrounding its splintering and ultimate creation of the domestic terrorist group the Weather Underground. SDS represents a significant social movement period for the United States and utilized the campus venue to incite political discourse about U.S. policy on a number of issues, including the Cold War, racial inequality, and Vietnam. In order to theorize about the potential security threat posed by hacktivist groups and web-based social movements and the potential metamorphosis of those groups into security threats, it is important to recognize the differences in activist organizations and the common or unique elements that enabled such civil rights organizations as SDS to evolve into a revolutionary terrorist group known as the Weather Underground. The SDS, as a loose and non-hierarchical organization is very reflective of today's hacktivist collectives and may potentially reveal characteristics consistent with transformation.

A. VENUE AS ORIGIN

In the early 1960s, a political movement emerged advancing a radically new critique of capitalism and the U.S. Cold War policy of nuclear deterrence and resulted not only in a shift in philosophical outlook but also in language and collective practice. The economic boom of the 1950s, although significant for the growth of Middle America, also isolated an impoverished and less influential minority segment of America. The poverty of the north and the segregation issues of the south influenced a civil rights movement that increasingly received attention from a minority number of students in prominent college and university campuses. Concurrent with the black lead civil rights movement, activists believed the anti-communist McCarthy era highlighted U.S. policy to rid the nation of communism in order to sustain a capitalist agenda seen as supporting a white elite. The anti-communist rhetoric also provided the U.S. government the rationale for nuclear armament that in the eyes of the student body increased the potential for conflict as evidenced by the Cuban missile crisis. Opposed to the centralized and

authoritarian politics of the Cold War, a loose collection of liberal, radical, and Marxist thinkers coalesced to form an American version of the New Left, a term already used to describe younger aged reformists in the United Kingdom and western Europe.[241] Members of the New Left believed that mainstream politics was dominated an elite who "preferred a docile public to an engaged one."[242]

The SDS emerged from a worker rights movement in 1960 when University of Michigan students, Alan Haber, Tom Hayden, and others who disenchanted by the narrow labor platform and lack of activism in America formed the SDS to highlight social and racial inequality in America. Shortly thereafter in 1962, SDS President Alan Haber conducted the group's first national convention in Port Huron, Michigan, where Tom Hayden released the group's first manifesto known as the Port Huron Statement.[243] Calling for a participatory democracy with decentralized decision making, the manifesto highlighted a number of issues to include racial and economic inequality in the United States, the Cold War tension, and threat of nuclear war. The document also highlighted its first call to action calling for a change in the political system based on non-violent civil disobedience. The statement's weaker stance against communism also served to isolate it from the workers party since SDS now viewed the Cold War and racism as their core issues.

Purposely intending the group to be an open society, as evidenced by its broad agenda enabled by participatory democracy, SDS leadership embraced the student body and campus venue for its inherent social reach and symbolism as a body for democracy. The campus venue also bridged the gap of funding and resource, a necessary component for the sustenance of any social movement.

---

241 Stuart Hall, "Life and Times of the First New Left," New Left Review, February 2010, http://newleftreview.org/II/61/stuart-hall-life-and-times-of-the-first-new-left.

242 Jeremy Varon, *Bringing the War Home* (Berkley, CA: University of California Press, 2004), 21.

243 Tom Hayden and Dick Flacks, "The Port Huron Statement at 40," The Nation, July 18, 2002, http://www.thenation.com/article/port-huron-statement-40#.

B. STRUCTURE

By espousing a campus movement, SDS disregarded a formal hierarchical system for a more autonomous base evolved from campus SDS chapters throughout the country.[244] However, for Haber, Hayden, and others, expansion would come at a cost to its hierarchical and national leadership since this broad approach to activism continuously threatened the ideological scope and purpose of the movement. This is a natural tendency for social movements since most movements do not necessarily possess authoritative leaders but rather leaders who, through the power of influence, control direction, and messaging for the movement.[245]

However, influential chapter presidents continuously exposed SDS's broad agenda to discourse effectively, which weaken the group's national leadership. The national office, attempting to appease the increased influence and power of the growing chapters, organized yearly SDS conventions where new national leaders would be elected. These conventions, consistent with its participatory model, were wrought with discourse about how to further its anti-imperialist agenda thus precluded any sort of successful decision making. The "work with all" approach failed to identify a true purpose other than to challenge the morality of the American system. Instead, SDS represented a "combination of ideas that challenged the existing social system."[246] This is significant since lack of ideology or purpose enables a number of influential members to swing or shift group agenda and thought towards different goals often resulting in sustained group discourse. In essence, SDS was a rather loosely drawn organization with relatively limited objectives. This broad agenda, although useful for increasing group membership, did not necessarily provide a strong core or anti-establishment argument and would ultimately serve as its biggest structural flaw.

---

244 Dana Zakrzewski, "Students for A Democratic Society," Campusactivism.org, accessed June 5, 2014, http://www.campusactivism.org/server-new/uploads/undergrad2a-sds.htm.

245 Lewis M. Killian, "Social Movement: Progressive Changes in Leadership and Membership," *Encyclopedia Britannica*, May 27, 2013, http://www.britannica.com/EBchecked/topic/551335/social-movement/25282/Progressive-changes-in-leadership-and-membership.

246 Geoff Bailey, "The Making of a New Left: The Rise and Fall of SDS," *International Socialist Review*, October 2003, http://www.isreview.org/issues/31/sds.shtml, 1.

C. DISCOURSE

Attempting to put "theory into action," SDS members formed a community outreach program called the Economic Research and Action Project to show solidarity with poor, mostly black communities and attempt to organize a poor people's movement.[247] SDS leadership hoped that this new movement would provide additional support for SDS and the then growing militant black power movement in the U.S. This proved to be short-lived as SDS organizers believed the power structure to be unresponsive of the demands from below, noting the slow and difficult nature of community organizing and the little social power inherent in the poor community.[248] According to Carl Oglesby, SDS President from 1965 to 1966, "If you really wanted to strike a blow against the war, you would be working on the campuses, because it was the campuses that were generating the enormous heat, the enormous pressure, the enormous growth, and really shaping the political."[249] This failed approach to align with the civil rights movement forced SDS to reorganize and search for new direction.

However, SDS's initial failure to galvanize the poor was soon replaced by another issue that would bring the movement in a new direction. In 1964, when North Vietnamese PT boats fired upon a U.S. naval destroyer vessel in the Tonkin Gulf, President Johnson and the U.S. Congress approved a resolution effectively authorizing increased U.S. military presence in Vietnam.[250] This government action strengthened the activists' belief that Vietnam was in fact an extension of American imperialist policy. The SDS student movement, personally impacted by the draft and America's policy in Vietnam, galvanized behind an anti-Vietnam War agenda. The campus environment provided real venue for campus sit-ins and candlelight vigils where increased radical rhetoric challenged America's imperialist policies. It is during this period that the SDS

247 Ibid., 3.

248 Varon, *Bringing the War Home*, 23.

249 Carl Oglesby, "It Was Like A Weed: Carl Oglesby on The 1960s Student Movement," December 12, 1984, http://historymatters.gmu.edu/d/6911/.

250 "U.S. Involvement in the Vietnam War: The Gulf of Tonkin and Escalation, 1964–1961–1968—Milestones—Office of the Historian," accessed June 5, 2014, http://history.state.gov/milestones/1961-1968/gulf-of-tonkin.

chapters evolved its tactics towards direct action that involved sit-ins and large protest marches.[251] The influx of new members and chapters surfaced the belief that SDS was a movement and not an organization thus should not be influenced by an elite few or bound by organizational discipline.[252] The SDS *brand* evolved into a decentralized structure that offered increased opportunity for chapters to advance utilizing strategies focused on the Vietnam War. By moving away from a hierarchical based organization towards a horizontal or flat movement, the SDS would became a "student power" movement focused on America's involvement in Vietnam.

Increasingly incensed with America's growing involvement in Vietnam and as a possible sign of solidarity with the student movement, SDS organizers, students, and teachers arranged teach-ins that included the burning of draft cards.[253] Student and faculty at the University of California at Berkley (UC Berkley) staged a series of protest movements during the 1964 fall semester that called for free political speech on campus and an end to the Vietnam War. At the time, UC Berkley and other academic institutions banned on-campus political activities, thus limiting the ability for students to effectively organize political movements. The UC Berkley protests symbolized a change in tactics towards direct action and were soon followed by a number of nationwide campus protest movements that were often confronted by police and local authorities.

In April 1965, the surge in SDS membership influenced leaders to organize a highly visible protest march in Washington, D.C., that caught the attention of government leaders and then Secretary Henry Kissinger, who commented that SDS was representative of the "main force on the white New Left."[254] The Port Huron Statement may have left the door open for competing ideologies; however, the Vietnam War became the unifying issue for SDS.

The anti-war protests effectively hijacked the SDS platform for a period of time between 1965–1968 increasing SDS's enrollment to approximately 100,000 students,

---

[251] Heath, G. Louis, *Vandals in the Bomb Factory* (Metuchen, NJ: The Scarecrow Press 1976).

[252] Ibid., 57.

[253] Ibid., 34.

[254] Ibid., 36.

many of whom were not aligned with the Port Huron statement or the New Left but rather drawn from the less radical working class directly affected by the Vietnam War. The Port Huron Statement was irrelevant to their purpose. This increased and diverse membership resulted in a new SDS convention that eradicated the Port Huron Statement and embraced an increasingly anti-communist agenda. The original, more socially focused members remained marginalized, increasingly frustrated with the direction of the movement. SDS, now fractured, lost its identity as a civil rights movement causing many to believe the organization's grassroots efforts were essentially over.

Noting this shift, then SDS President Carl Oglesby, during a speech at the SDS national convention in August 1966, stated that although there was a deep concern that something is wrong with America, "we need to develop greater clarity about what we think the world ought to be like."[255] The youth platform of SDS offered no political platform for change.

The SDS and activists behind the New Left movement were confronted with the realization that despite their perceived belief that the American system was imperialistic and served only the elite, in being unable to draw upon a victimized poor populace, it had very little chance of appealing to a comfortable middle class still benefiting from the capitalist American system.[256] The New Left "appeared to have reached the structural limit of its revolt."[257] By announcing itself as an anti-communist organization, the SDS had not only failed to align with a common radical collective but also left the door open for a number of competing ideologies to join the group. Chief amongst these was a fast growing student group called the Progressive Labor Party (PL), a pro-China Maoist party which had split from the old Soviet-oriented Communist Party of the United States.[258]

During the 1966–67 academic year, the now more autonomous SDS chapters evolved from "protest" to "resistance" and engaged in more harassing tactics such as

---

255 Ibid., 56.

256 Varon, *Bringing the War Home*, 45.

257 Ibid.

258 Mark Rudd, "The Death of SDS," Markrudd.com, accessed June 5, 2014, http://www.markrudd.com/?sds-and-weather/the-death-of-sds.html.

prolonged campus sit-ins, large protest gatherings, and marches and direct confrontations with campus draft boards. These resistance tactics, although passive, effectively disrupted university functions often requiring police intervention. The resulting confrontations with police, some notably violent, served to galvanize members of SDS and created new talking points of protest against an imperialist America.[259]

The following year, 1968, served as not only a tumultuous period for the U.S. with the assassination of presidential candidate Robert Kennedy and Martin Luther King, but also a turning point for the student organization. SDS chapters, "restless and frustrated" in the search for "instant change" began to encourage and engage in more disruptive activities such as draft resistance and campus takeovers.[260] Carl Davidson, the SDS national president, acknowledging the riotous tactics being employed by a national black power movement called the Black Panther Party demanded "either give us what we're asking for, or we'll shut this school down."[261]

In April of that same year, Mark Rudd, SDS chapter president at New York's Columbia University, noting perceived racial discrimination at a local Harlem, New York gymnasium and participation by a Columbia University think tank in a U.S. military weapons program, championed the direct action strategy and organized a campus wide sit-in that resulted in five university buildings being occupied and shut down for nearly one week.[262] Refusing amnesty for the student protestors, New York City police were called to clear the buildings, arresting more than 700 students with more than 100 students and a dozen police officers being injured in the confrontation.[263] Enraged by the forceful police actions, Columbia University students arranged a strike that caused the

---

259 Scott Midgley, *Peaceful Protest to Violent Revolution: The Evolution of SDS and the Weathermen* (Charles Town, WV: American Public University, 2011), http://www.academia.edu/1111206/Peaceful_Protest_to_Violent_Revolution_The_Evolution_of_SDS_and_the_Weathermen, 7.

260 Heath, G. Louis, *Vandals in the Bomb Factory*, 79.

261 Ibid., 84.

262 Margot Adler, "1968 Columbia Protests Still Stir Passion," *NPR*, April 23, 2008, http://www.npr.org/templates/story/story.php?storyId=89884026.

263 Robert McFadden, "Remembering Columbia, 1968," *New York Times*, April 25, 2008, http://cityroom.blogs.nytimes.com/2008/04/25/remembering-columbia-1968/.

campus to remain shut down for the spring semester. According to one of the protestors, the confrontations symbolized the beginning of militancy for the struggle allowing students to see "political conflict in overtly confrontational terms."[264] Subsequent to this event, campus flyers emerged that encouraged new battles utilizing such weapons as rocks, guns, firebombs, and plastique explosives.[265]

Robert Siegel, who worked as a reporter at Columbia University's radio station during the protest actions, recalled the effects of the police action stating that "some SDS members saw the sudden radicalization of kids who had been witnesses or victims of police brutality" adding "America was on the verge of revolution, they reasoned, provoke more Columbias, more police crackdowns, and then more radicals would emerge."[266] It is during this period that a smaller, more radical element began to take shape within SDS chapters.

One of the most enduring images of the SDS protest struggle occurred in August 1968 during the Democratic Party's presidential nominating convention held in Chicago.[267] SDS protestors, aligned with presidential candidate McCarthy's anti-war agenda, were confronted by a Chicago Police Department determined to prevent hundreds of SDS protestors from disrupting the convention. The police, utilizing blunt force tactics, engaged the protestors, many of whom were arrested and/or severely harmed by the police.[268] This direct confrontation with police not only symbolized the student struggle, but it also highlighted the limits of protest tactics against a stronger force.

D. FRACTURE

Consumed with an anti-war agenda, the decentralized SDS organization was no longer aligned with its original Port Huron socialist agenda and, outside of the Vietnam

---

264 Varon, Jeremy, *Bringing the War Home*, 26.

265 Ibid., 26.

266 Adler, "1968 Columbia Protests Still Stir Passion."

267 Wayne Heimbach and Bill Roberts, "A Look Back at the 1968 Democratic Convention," *International Socialist Review*, August 2008, http://www.isreview.org/issues/60/feat-chicago68.shtml.

268 Ibid.

War, still void of ideology. Seizing this opportunity, skilled organizers within the Progressive Labor Party (PL) quickly gained a foothold within SDS and received increasing support from the SDS chapters at Harvard University and other influential campuses.[269] Concerned about increasing influence from PL and disenchanted by the failure of the protest movement to effect U.S. policy in Vietnam, more radical and traditional SDS elements formed a separate faction called the Revolutionary Youth Movement (RYM) to vie for control of the SDS agenda platform.[270] As an opposing group to the PL, the RYM wished to recognize all student and working class Americans with the right to self-determination, a distinction not willingly granted by the PL. The PL faction, more aligned with communist ideology, saw the current working class as an "exclusive agent of revolutionary change" thus distinct from the student population.[271]

At the 1969 SDS National Convention in Chicago, members of the RYM famously submitted a new manifesto tilted "You Don't Need a Weatherman to Know Which Way the Wind Blows."[272] The manifesto announced the formation of RYM and outlined a transition strategy that would embrace third world revolutionary tactics in hopes of building a base of revolutionary minded SDS students that identified with anti-imperialist and anti-racist consciousness.[273] RYM, for the first time, offered an ideology-based direction for SDS.

Continuously aligned with the civil rights agenda, RYM members attempted to seize control of the SDS platform from PL and return SDS to its original socialist agenda of equality. RYM, whose leadership members included SDS chapter leaders Mark Rudd from Columbia University, Bill Ayers from the University of Michigan, and influential newcomer Bernadine Dohrn from the University of Chicago, all of whom were aligned with the revolutionary Black Panther Party movement were able to orchestrate a vote that

269 Rudd, "The Death of SDS."

270 Varon, *Bringing the War Home*, 46–49.

271 Ibid., 46.

272 Karin Asbley et al., "You Don't Need A Weatherman To Know Which Way The Wind Blows," June 18, 1969, https://archive.org/details/YouDontNeedAWeathermanToKnowWhichWayTheWindBlows.

273 Ibid.

successfully removed the popular PL faction from SDS.[274] The success of their effort effectively denied a majority of SDS chapters of its chosen Maoist platform. Now unopposed, RYM became the leading body within SDS and, in reference to their manifesto, became known as the Weathermen.

The fracture and subsequent takeover of SDS by a minority sect was significant. In his thesis studying the path towards terrorist violence, Dean Olson notes that political violence is often a byproduct of ineffective or failed social movements. According to Olson, "the development of a revolutionary dimension and increased risk of violence occurs when various factions begin to fragment along ideological lines over disagreements about what methods to employ to achieve goals."[275]

Disenfranchised by the ineffectiveness of the anti-war movement and "arm-chair Marxism," RYM attempted to reinvigorate the SDS civil rights and social inequality platform by calling for a Day of Rage in Chicago to coincide with the opening of the trial for a group of demonstrators arrested the previous for their participation in protests at the Democratic Convention.[276] The defendants, known as the Chicago 8, also included an influential Black Panther Party leader Bobby Seale. Inspired by the confrontational tactics of the Black Panther Party, the Weathermen called upon SDS members to join forces in a violent struggle to avenge the violent police tactics used against them during the Democratic Convention. During a three-day period in October 1969, Weathermen members, donning helmets gas masks, and blunt force weapons, such as sticks and pipes, repeatedly engaged the Chicago police, engagements which resulted in a number of arrests and serious injuries.[277]

However, rather than galvanize the SDS membership, according to Heath, the Day of Rage protest failed to garner large support and in fact served to further isolate the Weathermen from the SDS base who questioned their tactics. The one thing the riotous

---

274 Rudd, "The Death of SDS."

275 Dean T. Olson, "The Path to Terrorist Violence: A Threat Assessment Model for Radical Groups at Risk of Escalation to Acts of Terrorism" (master's thesis, Naval Postgraduate School, 2005), 14.

276 Rudd, "The Death of SDS."

277 Heath, *Vandals in the Bomb Factory*.

Day of Rage tactics did do was establishing the Weathermen as a threat to society. The failure to garner the support of the student movement exposed the Weathermen's mass revolutionary strategy as flawed. The remaining members of the Weathermen, estimated at no more than 150 people, were forced to find new ways to continue their struggle.[278]

In December 1969, in Flint, Michigan, the Weathermen held its last public meeting, now referred to as the "War Council." The result of the meeting was a new clandestine group called the Weather Underground Organization (WUO) and a declaration of war by Bernadine Dohrn that effectively marked the group's transgression to terrorist bombing tactics. Forced to retreat underground, the WUO utilized a cell structure aligned with the group's ideology and commitment towards terrorist bombing tactics. Already a target for law enforcement, including the FBI, the group's clandestine structure was essential for survival.

However, the Weathermen's terrorist tactics were challenged early in their campaign. In 1970, New York based Weathermen, in an attempt to build anti-personnel devices to target a dance at the Fort Dix Army Base in New Jersey, accidentally initiated the device killing three of the five Weathermen present in the apartment.[279] The subsequent public and media outrage forced WUO leaders, known as the Weather Bureau, to debate their own tactics and the ethics of targeting human life as part of their terrorist campaign.[280] The group decided to avoid targeting human life but rather the symbols of the "imperialist U.S. government" and proceeded with a multi-year bombing campaign that targeted the U.S. Capitol Building, the Pentagon, and others symbols of authority, such as the New York City Police Headquarters building. The selective targeting campaign was intended to garner support and maximum attention without further alienating itself from the mass. By drawing attention to their cause, perhaps a silent majority would self-radicalize and embrace WUO's less than lethal tactics.[281]

---

278 Ibid.

279 Ibid., 174.

280 Ibid., 182.

281 David Ucko, "The Weather Underground: A Different Approach to Political Violence," KingsOfWar, January 26, 2011, http://kingsofwar.org.uk/2011/01/the-weather-underground-a-different-approach-to-political-violence/.

However, their use of restrained bombing tactics still made them indistinguishable from more deadly terrorist groups, thus drawing them into a protracted war of attrition with the U.S. government they would ultimately lose.

E. CONCLUSION

As a campus based movement, SDS's broad socialist agenda highlighted a number of social causes most notable of which was segregation and poverty. The increasing involvement of the U.S. in the Vietnam War served as a catalyst for the growth of the SDS movement beyond its northern-based campus presence. These new chapters or clusters, void a specific ideology or purpose, were able to frame the debate at the local level resulting in increased discourse at the yearly SDS national conventions. The increasing anti-war sentiment in the midwest and southern chapters resulted in an SDS base largely concerned with the Vietnam War and not the underlying SDS anti-imperialist agenda. The founders' desire for a participatory democracy as outlined in the Port Huron Statement shifted SDS from an organization to a brand to be interpreted by the individual chapters. Thus, the campus venue, effective for mass gathering and communication, also proved difficult to control since. Aside from the national conventions, SDS national leaders could no longer control the message and relied upon the influence and allegiance of its chapter leaders. This important finding possibly reflects the challenge of formulating and directing social movements web-based via the Internet's communication platforms, since like the campus venue, social media is an open venue where users can openly express opinion and commentary. Hacktivists intent on change may be frustrated by the continuous discourse on the web finding it difficult to formulate and maintain an idea or identity.

According to McCormick, this lack of popular support for the group's political agenda in an otherwise permissive environment places decision makers at odds with each other, thus directly impacting the strategic environment of other factions like the Weathermen.[282] As previously noted, clusters, or in this case the individual SDS

[282] Gordon H. McCormick, "Terrorist Decision Making," *Annual Review of Political Science* 6 (June 2003): 482.

chapters, become cognitive layers within the larger discourse. The autonomous structure allowed for a horizontal decision-making process not subject to hierarchy or hegemonic authority. This structure makes the larger collective vulnerable since, as in the case of the Weathermen, transgressors "seek ways to free human individuality from the bonds of representation that would contain it."[283] The open and democratic nature of Anonymous suggests that those more skilled or passionate members, unable to elevate their ideas, will undoubtedly retreat from the larger collective to form smaller clusters or cells of likeminded individuals.

However, the actions by RYM to remove PL from the SDS Convention platform in 1968 resulted in a RYM leadership position based upon weak bonds since the majority of the SDS base aligned with the PL Maoist agenda. These weak ties resulted in decreased support and action ultimately requiring the strategy of chaos and disruption.[284]

In attempting to isolate triggers for the emergence of the Weathermen, it is necessary to examine a number of factors over a period of time. Leaders of the Weathermen became increasingly frustrated with the ineffectiveness of the protest movement and success of police intervention. In this sense, it is possible to view the perceived disproportionate reaction of the authorities towards numerous SDS demonstrations as influential towards the use of more revolutionary tactics. The Columbia University incident was just one of many clashes with police that ultimately culminated in the nationally televised and brutal confrontation between SDS protesters and the Chicago Police Department at the 1968 Democratic Convention. The subsequent appearance of campus protest flyers calling for use of weapons and explosives were significant indicators of building frustrations and move towards transgressive action. This is significant since global law enforcement efforts against hacktivists have increased with notable voices of resistance.[285]

---

283 Foust, *Transgression as a Mode of Resistance*, 209.

284 Piven and Cloward, "The Weight of the Poor: A Strategy to End Poverty."

285 John Knefel, "Cyber-Activist Jeremy Hammond Sentenced to 10 Years in Prison," *Rolling Stone*, November 15, 2013, http://www.rollingstone.com/politics/news/cyber-activist-jeremy-hammond-sentenced-to-10-years-in-prison-20131115.

The stated Weathermen ideation as noted in the release of their manifesto was distinct since it acknowledged factional support behind a purpose and ideology beyond the Vietnam War ultimately forcing a break from the base. In this context, the move towards terrorist tactics was not the product of a single decision but rather the "end result of a dialectical process" that gradually pushed the Weathermen toward a commitment of violence.[286] According to McCormick, a person can arrive at this end state from a number of different starting points, as exemplified by the differing SDS tenures and geographic base of Weathermen members.

However, the failed Day of Rage actions by the Weathermen already resulted in their becoming increasingly isolated from the SDS base. Increased confrontations with law enforcement only exacerbated a need for an increasingly violent organization to move underground. The move underground not only represents a flight to safety but also a predominant advantage for groups wishing to implement a strategy of subversion. SDS' open platform and hierarchical structure was vulnerable to discourse and infiltration. Terrorist groups wanting to survive must become clandestine organizations. Thus, this apparent desperate and isolating move, although consequentially removing the group from its larger SDS base, also offered a layer of resilience that enabled it to carry out a multi-year bombing campaign. Anonymity is a significant advantage for any adversary and is an inherent trait of the Internet.

[286] McCormick, "Terrorist Decision Making," 492.

VI. EARTH FIRST!

In the 1990s the Earth Liberation Front rose to infamy as a domestic terrorist group responsible in part for more than $100 million in damage to corporate land developments and businesses.[287] However, radical environmentalist groups such as ELF were not idly born but rather evolved from the environmentalist social movement of the late 1960s and 1970s. One such movement called Earth First! spawned the concept of direct action under the veiled cover of a decentralized cell network all the while carrying the public message to save the Earth. Despite the popularity and acceptance of environmentalism, members of Earth First! evolved into more radical collectives responsible for hundreds of crimes and acts of terrorism that included arson, bombings, vandalism and harassment. Despite increased pressure, Earth First! and ELF have sustained and remain resilient to law enforcement actions against it. In order to understand how web based movements may shape and sustain, this chapter will focus on the evolution of the radical environmental movement Earth First! and associative organizational structure to identify factors involving the resiliency of autonomous movements. The autonomous cell structure, although resilient, also appears difficult to govern and possibly enables increased discourse within radical organizations.

A. ORIGINS

In the early 1960s, a political movement emerged that criticized environmental practices and was "characterized by not only a shift in philosophical outlook, but also in language and collective practice."[288] This period is often associated with the founding of the deep ecology framework, authored by Norwegian philosopher Arne Naess in 1972. Deep ecology asserts that all objects in nature have intrinsic worth and should enjoy special status in the world.[289] Proponents for this philosophy believe that all objects in

---

287 "FBI: Eco-Terrorism Remains No. 1 Domestic Terror Threat," *Fox News*, March 31, 2008, http://www.foxnews.com/story/2008/03/31/fbi-eco-terrorism-remains-no-1-domestic-terror-threat/.

288 Loadenthal, "The Earth Liberation Front," 18–19.

289 Donald R. Liddick, *Eco-Terrorism: Radical Environmental and Animal Liberation Movements* (Westport, CT: Praeger, 2006), http://sinzoofilikon.weebly.com/uploads/5/0/5/7/5057569/animal_terrorism.pdf, 3.

nature are intertwined and essential to the survival of earth's ecosystem. Disruption or harm to the environment fueled the belief that an "environmental apocalypse is imminent."[290] It is this entwined belief that fueled a new philosophical movement of environmentalism away from a political solution towards a spiritual one. Inspired by this new radical shift, a small group of environmentalists for the first time justified the use of illicit and/or criminal acts in defense of the earth.

Concurrent with this philosophical shift was an increase in conservative American policy that favored economic growth resulting in the Department of Agriculture agreeing to open up millions of acres of federally protected land for use by the timber and oil industry.[291] Frustrated by this decision and the lack of outrage by mainstream environmental groups, lobbyist David Foreman and other discouraged environmentalists formed an environmental activist group called Earth First!(EF).[292] In defending the environment, the group believed extra legal tactics were necessary to fulfill their promise of "no compromise in the defense of Mother Earth."[293]

Aligned with the framework of deep ecology and deeply influenced by Edward Abbey's 1975 novel *The Monkey Wrench Gang*, Earth First! employed a variety of rhetorical strategies to realign public opinion and policy on environmental issues.[294] In his fictional book, Abbey highlighted the use of sabotage to disrupt logging efforts against the southwest forest region.[295] Inspired by this rhetoric, Earth First! unfurled a 300-foot black plastic banner down the face of the Glen Canyon Dam in Arizona.[296] The

---

290 Ibid.

291 Ibid.

292 Marilyn Cooper, "Environmental Rhetoric in the Age of Hegemonic Politics: Earth First! And the Nature Conservancy," in *Green Culture: Environmental Rhetoric in Contemporary America*, ed. Carl G. Herndl, Stuart C. Brown (Madison, WI: University of Wisconsin Press, 1996), 238.

293 Emily N. Jackson, *Environmental Direct Action: Tactics for Environmental Policy Change*, Indiana University-School of Public and Environmental Affairs, 2013, http://www.indiana.edu/~spea/pubs/undergrad-honors/Volume-7/Jackson,%20Emily%20-%20Environmental%20Direct%20Action-Tactics%20for%20Environmental%20Policy%20Change%20-%20Faculty%20Sarah%20Mincey.pdf, 11.

294 Cooper, "Environmental Rhetoric in the Age of Hegemonic Politics," 238.

295 Edward Abbey, *The Monkey Wrench Gang* (New York: Dream Garden Press, 1985).

296 Daniel J. Philippon, "Edward Abbey's Remarks at the Cracking of Glen Canyon Dam," *Oxford Journals: ISLE* 11, no. 2 (2004): 161.

contrast of the black banner against the concrete wall of the dam offered a visual that suggested the dam was cracking. With the spotlight now on Earth First!, the group gained notoriety as a mobile and action oriented movement whose members converged on targeted areas and, upon concluding their actions, returned home to form other Earth First! oriented groups.[297] This simple act of aggression, though harmless, effectively elevated attention and awareness of the group providing it a platform for recruitment. In a sense, the group's cause determined its venue since the ideological focus was the earth itself.

B. STRUCTURE

Although founded by David Foreman, Earth First! had no central authority but rather resembled the autonomous cell structure proposed by Abbey's in his fictional novel. In the book, activists discussed plans for a disorganized movement composed of small groups of anonymous cells that perpetrated economic sabotage throughout the nation.[298] As the influential and founding member of Earth First!, Foreman exercised public control of the group's messaging and initially its action via an autonomous cell structure loosely connected via the group's quarterly publication called the *Earth First! Journal*. An important method of communication, the *Earth First! Journal*, was touted by editors as "an essential forum for discussion within the Earth First! movement."[299] It is in this structure that Foreman hoped to shape the actions and ideology of the movement.

Anti-government activist Louis Beam in his article entitled "Leaderless Resistance" memorialized the use of clandestine, decentralized networks of autonomous cells as a means of resistance against tyrannical states. According to Beam, hierarchical organizations are ineffective against advanced enemies and have been historically penetrated by government agents. The strategy of leaderless resistance employs small groups or cells that "fight an entrenched power through independent acts of violence and

297 Jackson, "Environmental Direct Action," 12.

298 Abbey, *The Monkey Wrench Gang*.

299 "About the Earth First! Journal," *Earth First! Journal,* accessed June 12, 2014, http://earthfirstjournal.org/about-the-earth-first-journal/.

mayhem."[300] Absent direct command or a hierarchical leader, the leaderless cells are unable to communicate with each other thus maintain the advantage of anonymity, a key component for success and security. Although the autonomous structure lacks command, it does not necessarily imply lack of cooperation.[301]

According to Liddick, because underground activists remain anonymous and isolated, "their success depends critically on aboveground members in the movement, who provide support and direction."[302] Thus, above ground operations are important to provide the proper messaging and legitimacy to the given movement all the while communicating agendas to underground operatives.[303] Earth First! effectively achieves this through its publication of the *Earth First! Journal.* For Foreman, the journal provided an important communication channel to provide direction, disseminate information, and inspire underground activists with the benefit of deniability for subsequent cell actions. The journal also served as a source for activists to critique and discuss actions of the environmental movement and engage in discourse about the direction of the group. This form of communication, though consistent with the types of materials used by SDS, such as pamphlets, leaflets, and magazines, demands the important and scarce equity of time and resource. The ubiquitous nature of web-based social media platforms not only transcend this need but also provide vast outreach ability.

As anonymous entities, Earth First! cells are influenced by the discourse and changing dynamics available via the *Earth First! Journal*. This effective outreach mechanism provides effective leadership and communication at minimal costs for the organization. Thus, above ground leaders, like Foreman, are able to remain engaged in the politic and attempt to bring new ideas to the masses. By playing the role of the intellectual, Foreman is committed to legitimizing the environmental movement with the

---

300 Simson L. Garfinkel, "Leaderless Resistance Today," First Monday, March 3, 2003, http://firstmonday.org/ojs/index.php/fm/article/view/1040/961.

301 Ibid.

302 Liddick, *Eco-Terrorism: Radical Environmental and Animal Liberation Movements*, 69.

303 Ibid., 70.

tangential support of the underground movement.[304] According to Eyerman and Jamison, such overt efforts to elevate environmentalist movement into scientific discussion or "knowledge making" are an inclusive process known as cognitive praxis.[305] Social movements, like Earth First!, combine science, thought, and action to further their cause—ultimately forming a "collective identity" behind the movement. The above ground leaders are required to institutionalize the movement if it is to survive as a legitimate organization. However, as the above ground leader, Foreman is the most visible and, by default, most vulnerable member of the group.

C. DISCOURSE

Formed as a direct action group, Earth First! intended to raise awareness of the environmentalist cause and directly challenge pro-industry policy in this area. Although worldviews on environmentalism suggest adherents have a "moral obligation to vigorously protect all eco-systems and those living within it;" deep ecologists believe that humans are the cause of massive death and destruction to life, therefore, "must be targeted and persuaded to change."[306] However, from its onset, Earth First! declared itself as an activist group dedicated to using non-violent direct action tactics focused on disrupting industry logging efforts. This was achieved via highly visible protest actions that utilized such tactics as tree sit-ins, blockades, and sabotage. Effective tree sit-ins were analogous to wars of attrition where protestors would sit in trees targeted for removal by the logging industry. These actions sometimes lasted for weeks and usually required police intervention to facilitate their removal.[307] Likewise, other members chained themselves to heavy machinery such as bulldozers to prevent their being used until their forced removal.

---

304 Ibid.

305 Andrew Jamison, "Social Movements and Science: Cultural Appropriations of Cognitive Praxis," *Science as Culture* 15, no. 1 (2006): 47.

306 Jackson, "Environmental Direct Action," 7.

307 Andrew Christensen, "Squaw Three Trespass," Pendbay, August 8, 1985, http://www.penbay.org/ef/ronfedstatements85.html.

These passive resistance tactics were aligned with the philosophy of deep ecology and the need to ensure that no harm comes to human or non-human life. Ascribed to this belief, Foreman and early Earth First! members took care to refrain from confrontational or harmful actions. Although the unfurling of the banner at Glen Canyon Dam appeared to most as a stunt, these tactics effectively highlighted the group's message and increased the its ability to attract adherents and obtain funding.

Many Earth First! activists were arrested for relatively minor offenses during these early protest actions; however, their actions also had the positive effect of attention and empathy to their cause. Increasingly agitated, loggers became confrontational with the protesters and, on one occasion, Foreman was run over by loggers in a pick-up truck causing permanent damage to his knee.[308] Despite this aggressive challenge, Foreman initially resisted elevating Earth First! protest tactics. However, despite their passive protest efforts, Earth First! members received harsh fines and jail time in contrast to the lenient actions against confrontational loggers. Foreman, now limited by his injury and discouraged by the failure of the group's efforts to alter policy, advocated elevating direct actions to include "monkeywrenching" or tactics that included burning heavy equipment and tree-spiking.[309]

In 1985, Dave Forman published *Ecodefense*, a direct action or "monkeywrenching" manual that laid out the principles for utilizing direct action.[310] Insisting that monkeywrenching tactics are non-violent and ethical actions, Foreman provided detailed instructions for tactics, such as decommissioning bulldozers, removing survey stakes, and tree spiking. These actions were portrayed as a way to halt deforestation and development and provide activist groups like Earth First! the opportunity to elevate and create discussion around targeted issues.[311] However, acts of

---

308 Christopher J. Covill, *Greenpeace, Earth First! And The Earth Liberation Front: The Progression of the Radical Environmental Movement in America* (Kingston, RI: University of Rhode Island, 2008), http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1095&context=srhonorsprog, 41.

309 Ibid., 42.

310 Dave Foreman and Bill Haywood, *Ecodefense: A Field Guide to Monkeywrenching*, 3rd ed. (Ann Arbor, MI: Abbzug Press, 1993).

311 Ibid.

monkeywrenching can range from benign to the potentially very dangerous. The so-called passive acts of machinery torching and physical removal of parts contrasted against the potentially harmful effects of tree-spiking. In 1987, a mill worker was seriously injured when a saw he was operating was shattered by a tree spike, an act which immediately drew increased attention to the group.[312] The injury forced Congress and national forest supervisors to reevaluate the danger posed by environmentalists resulting in new policy that authorized denying access to national forests whenever environmental protests were expected.

D. FRACTURE

The autonomous structure of Earth First! comprised of both above ground and below ground members and, although highly effective at shielding identity and responsibility for criminal actions, also required an open framework for discussion. This open door policy, much like that of the Students for a Democratic Society, was vulnerable to being hijacked by aggressive discourse. Members were able to express diverse opinions via written publications such as the *Earth First! Journal* and used such venues to challenge the effectiveness of their tactics. Inspired by the publication of Foreman's *Ecodefense* and the more aggressive tactics of torching and tree-spiking, Earth First! membership was increasingly and unwittingly drawn from left leaning Marxist and anarchists who increasingly advocated the use of such ecotage tactics as arson and vandalism.[313] As a direct action group, Earth First! was increasingly blamed for actions it did not commit.[314] Concerned with the increasingly violent direction of the group, Foreman attempted to return Earth First! to its original passive style. However, newer members, already maddened by the violent actions of the loggers, opposed Foreman and, utilizing the communication platform of the *Earth First! Journal*, proposed sustaining the use of violent direct action tactics.[315]

---

312 Covill, *Greenpeace, Earth First!*, 46.

313 Ecotage is an environmentalist term for the use of sabotage tactics in furtherance of an ecological cause.

314 Covill, *Greenpeace, Earth First!*, 49.

315 Ibid.

Foreseeing the increasingly violent discourse within the movement, Foreman offered members who opposed the increasingly violent tactics monkeywrenching and direct action a "no fault divorce" from the group resulting in some members pursuing other nonviolent environmental causes.[316] Foreman's belief that Earth First! could somehow remain detached from the activities of the underground cells was unrealized as their actions were increasingly associated with the public face of Earth First! By maintaining his belief that Earth First! could influence public opinion via non-violent means, Foreman fractured the group's collective identity, previously composed of autonomous networks for direct action. Frustrated by the group's inability to impeding urban sprawl, radical members believed that the environmental movement required more subversive tactics of "ecotage" that included acts such as arson and sabotage. Discourse, once elevated, provided a measure of internal and external conflict that influenced the direction of the movement. By the late 1980s, Earth First! had become synonymous with direct action and the increasingly violent environmental movement. Increased occurrences of sabotage against machinery and torching of home projects were publicly attributed to the group regardless of genuine attribution.

An FBI investigation of Earth First! Arizona resulted in numerous arrests of the group's members, including Foreman himself who was charged with conspiracy involvement in a series of sabotage attacks against a ski resort and power transmission lines. Foreman was eventually charged with a misdemeanor and $250 fine; however, the FBI actions signaled a growing interest in the group's activities.[317] Foreman's effort to retreat from his rhetoric was directly challenged by an increasingly radical membership desiring more disruptive direct action. This challenge response mechanism was also represented in the Weathermen's initial reactions to SDS encounters with the Chicago Police Department. However, the Day of Rage failed to galvanize the SDS behind the group's more radical tactics and instead served to isolate its members from the student body. As previously discussed, SDS's broad agenda failed to coalesce the movement; on

316 Ibid.

317 Ibid.

the other hand, the ideological cause of environmentalism ensured a passionate and purposed following.

Challenged with the left leaning movement of the group and law enforcement efforts to disrupt their activities, Foreman attempted to align Earth First! with mainstream environmental groups that were more engaged in public discourse and non-violent protest actions. Judi Bari, an original founding member of Earth First! and well-known feminist, disagreed with Foreman regarding the moderate use of direct action. While driving in her car as part of an organizing campaign to save the Redwoods of northern California, Bari was nearly killed by a pipe bomb suspected of being planted by members of the timber industry.[318] Still opposed to Foreman's passivity, Bari encouraged left leaning Earth First! members to leave the group and join the then nascent and more radical Earth Liberation Front (ELF), a radical environmental group emerging out of the United Kingdom (UK).[319] In the September–October 1993 issue of the *Earth First! Journal,* an anonymous article announced the creation of the ELF. It stated that the ELF "is a movement of independently operating eco-saboteurs" that split from the British Earth First! movement, which has focused directly on public direct actions.[320] Having lost the message, Foreman could no longer control the direction of the autonomous network and feeling "uncomfortable and out of place in their own group," disgruntled members severed ties with Earth First! in 1990.[321]

The Earth Liberation Front itself was a merger of environmentalists and England's already popular Animal Liberation Front (ALF), a group that used destructive tactics of arson, bombing, and vandalism to intimidate corporate entities that profited from the perceived abuse of animals. Since many members of Earth First! were discouraged by the ineffectiveness of the group's non-violent direct action tactics, the UK's ELF represented an opportunity to align with likeminded activists across the

---

318 Ibid.

319 Ibid., 58.

320 "Earth Liberation Front (ELF)," TargetOfOpportunity.com, accessed June 16, 2014, http://www.targetofopportunity.com/elf.htm.

321 Covill, *Greenpeace, Earth First!*, 60.

Atlantic. Already feeling the pressure from law enforcement throughout Europe, the chance to align with American counterparts increased the group's resiliency and the safe haven of an autonomous network in the United States.

On Columbus Day, October 14, 1996, in their first attack inside the United States, members from ELF, wanting to redress the "oppression of indigenous people everywhere," attacked symbols of corporate America by targeting a Chevron gas station, a public relations office, and a McDonald's restaurant by gluing the locks to each facility and painting the property with political messages and the three letters E.L.F.[322] Since that initial attack, ELF has gone on a violent multi-year campaign that has included burning down a Vail, Colorado ski resort, a logging headquarters, multiple housing developments, sport utility vehicle dealerships, and also the detonation of a gasoline bomb at Michigan State University (an apparent protest of the university's genetic engineering research).[323] According to the FBI, ELF's criminal tactics of vandalism and arson are responsible for causing over $100 million in property damage.[324] The U.S. government has declared ELF as "the most active criminal extremist element in the United States" and "number one domestic terrorist threat."[325] Today, the ELF remains active, transitory and, due to its decentralized, clandestine and autonomous structure, resilient to authority.

E. CONCLUSION

Despite U.S. efforts to disrupt radical environmental activist efforts, the Earth First! and ELF movements remain notable and recognizable on a global scale. Foreman's introduction of direct action tactics to a decentralized organization not only resulted in raising the public consciousness of environmentalism but also attracting the attention of authority. As a decentralized organization, Earth First!'s founder Forman effectively maintained an above ground persona that could argue environmental issues while distancing himself and others from the actions of the underground network. Earth First!

322 Loadenthal, "The Earth Liberation Front," 16.

323 "Fanning the Flames!," *Do or Die*, no. 10 (2003): 137–39.

324 "FBI: Eco-Terrorism Remains No. 1 Domestic Terror Threat," *Fox News*.

325 Loadenthal, "The Earth Liberation Front," 16.

never publicly took credit for its monkeywrenching tactics but rather gained sympathy through it publications and more peaceful protest actions. This structure, though effective for self-preservation, also left the group vulnerable to increased radical action as evidenced by the discourse in the *Earth First! Journal* articles and autonomous cell actions. However, as Foreman realized, once accepted, ideologies are difficult to refrain.

Perhaps spooked by his arrest or inability to wrest control of the Earth First! movement, Foreman ceased acting as the aboveground leader for Earth First!, and he went on to create the Wildlands Project and serve on the board of the Sierra Club, both environmental think tank organizations. However, his departure from Earth First! did nothing to impact the radical environmental movement. Today, there are several hundred Earth First! related organizations around the world.[326] According to activist Darryl Cherney, "Many Earth First!ers have actually gone on to start new organizations with much stronger 'no compromise' positions."[327]

"Earth First! is a verb, not a noun."[328] This poignant statement reflects the resiliency of not only movements but also the ideology behind them. According to Loedenthal, names such as the ELF, ALF (a popular animal liberation group closely aligned with ELF in politics and tactics), and Earth First! "are freely adoptable political markers providing little more than an articulation of a shared politic and recognizable name."[329] The idea itself becomes the collection platform.

According to Ingalsbee, environmental movements like Earth First! represent new forms of collective identifies that attract activist communities. The new activist identities form a collective consciousness for action.[330] The *Earth First! Journal* or today's social media platform provide "temporary liberated zones where dominant discourses and cultural norms can be symbolically countered, and alternative discursive practices –such

326 "Earth First!—Activist Facts," Activist Facts, accessed June 16, 2014, https://www.activistfacts.com/organizations/271-earth-first/.

327 Ibid.

328 Ibid.

329 Loadenthal, "The Earth Liberation Front," 41.

330 Timothy Ingalsbee, "Earth First! Activism: Ecological Postmodern Praxis in Radical Environmentalist Identities," *Sociological Perspectives* 39, no. 2 (1996), 272.

as identity- can be socially created."[331] Thus, much like the SDS before them, autonomous structures like Earth First! represent ideological platforms that morph into unforeseen and at times radical new identities that are resistant to technocracy.

331 Ibid., 272.

VII. ANONYMOUS

Over the past decade, a number of hacktivist groups have demonstrated their disruptive abilities utilizing the cyber platform. Many of these groups still sustain today and have active members willing to openly and publicly participate in social discourse. However, one of the most disruptive and controversial of all of these groups chooses to engage anonymously as a collective known as Anonymous. Unlike other hacktivist groups such as Electronic Theatre, whose members and leaders are openly engaged in discussion, members of Anonymous remain true to their moniker and, like many social movements before them, embrace anonymity as a necessary and essential characteristic of their cause. As a non-hierarchical collective, Anonymous bears similarities to the SDS and Earth First!, not only in structure but also its vulnerabilities of discourse and radical behavior. This chapter will review the evolution of Anonymous as a web-based social movement and identify unique and distinctive characteristics that, if uninterrupted, may enable this collective to become an increasingly disruptive force and security concern for the homeland.

A. ORIGINS

On October 1, 2003, a simple image based bulletin board started by a 15-year old in New York City received its first innocuous post by a user known only as "moot." The board, 4chan, intended to host conversation around various anime and other comic based media, became very popular for its free cost and ability to post anonymously, an attractive feature for lurkers and posters. Those posters who wished to use the message board and not identify themselves were labeled only as "Anonymous."[332] In fact, 4chan, an online forum, in recognition of the favorable characteristic of anonymity, describes "Anonymous" as "not a single person, but rather, represents the collective whole of 4chan."[333] This is an important distinction since research suggests that, behind the mask, people are willing to engage more freely on divisive subjects without the threat of

332 "4chan—FAQ," 4chan, accessed July 25, 2014, http://www.4chan.org/faq#anonymous.

333 Ibid.

retribution or ridicule.[334] The opinions of posters are objective and usually unbiased since unidentifiable posters cannot be isolated on the web by the members. The increasing popularity of the site caused the board to evolve from its intended focus into other message groups for random thought or discussion and soon resulted in 4chan becoming a full-fledged online community with nearly 18 million monthly users.[335]

As previously discussed, online communities represent platforms for communication and discourse often resulting in clusters formed around similar ideas and issues. This was also true for 4chan as early users. They were comprised mostly of younger computer savvy members who, via 4chan and other Internet Relay Chat services, began to formulate loosely connected groups centered mostly on mischief and, in their words, "lulz." a commonly used Internet phrase meaning "fun, laughter, or amusement" usually at another's expense.[336] According to Quinn Norton, journalist for *Wired* magazine, "lulz is laughter with pain in it" and "forces you to consider injustice and hypocrisy, whichever side of it you are on in that moment."[337] For Anonymous, "lulz" is the reason for being as it requires action when times are tough.[338]

These clusters, though formed from open online communities, can formulate their own identities based upon rhetoric and action and, as a result, constrict its members to those willing to embrace their actions. This unintended consequence resulted in 4chan becoming a critical communication platform for likeminded hackers wishing to use their computer skills for mischief.

In what is considered one of its first actions as a loosely organized collective, the "anonymous" members of a 4chan message board called "/b/" organized a large-scale

---

334 Philip Zimbardo, *The Lucifer Effect: Understanding How Good People Turn Evil* (New York: Random House Trade Paperbacks, 2007), 25.

335 Alexia Tsotsis, "4Chan Has 18M Uniques A Month, Canvas Participation Is Optional," TechCrunch, May 25, 2011, http://techcrunch.com/2011/05/25/4chan-has-18m-uniques-a-month-but-canvas-participation-is-optional/.

336 *Oxford Dictionaries*, s.v. "Lulz," accessed July 24, 2014, http://www.oxforddictionaries.com/us/definition/american_english/lulz.

337 Quinn Norton, "Anonymous 101: Introduction to the Lulz," *Wired*, November 8, 2011, http://www.wired.com/2011/11/anonymous-101/all/1.

338 Ibid.

"raid"[339] in July 2006 against a Finnish social networking site called Habbo.[340] One of Habbo's virtual communities known as Habbo Hotel was "raided" by members of Anonymous who, by placing numerous dark skinned avatars around the site's virtual poolside, restricted entry to participants who were informed that the pool was "closed due to AIDS."[341] Anonymous' actions were an apparent response to Habbo site moderators alleged tendency to ban users based upon the skin color of their avatars. Although the Habbo raid was orchestrated for the lulz, it reflected for the first time the unique ability of community message boards to quickly swarm and formulate action. Anonymous evolved as a loosely organized collective from 4chan and exemplified the capability of web based collective action. Although limited, the media coverage of the event highlighted the power of social media in organizing Internet raids with little resource. This is meaningful since the members of Anonymous were largely unknown to each other and still void of the philosophical or ideological direction consistent with previously discussed social movements.

Now established as a collective, in 2006, Anonymous still in search of lulz and in its first foray into activism, famously targeted the website of white supremacist and radio talk show host Hal Turner. Primarily using DDoS tactics, Anonymous knocked Turner's website offline causing thousands of dollars in damage and lost revenue to Turner who would later unsuccessfully attempt to sue 4chan and other community host websites for their actions.[342] Perhaps more damaging, some members of Anonymous successfully exfiltrated email data from Turner's server network that revealed Turner as a confidential informant for the FBI, thus impinged upon law enforcement efforts and caused personal risk to Turner.[343]

---

339 A "raid" is a common term for an organized assault on a website or forum by a group of web-based agitators such as Anons, normally designed to cause disruption on a large scale.

340 Tomberry, "Pool's Closed," KnowYourMeme, accessed July 22, 2014, http://knowyourmeme.com/memes/pools-closed.

341 Ibid.

342 Anthony Olszewski, "Internet War Waged against Hal Turner, New Jersey Hate Monger," Free Republic, December 28, 2006, http://www.freerepublic.com/focus/f-news/1759563/posts.

343 Dana Edwards, "The Internet Vigilante Mob, Justice or Internet Vigilantes Run Amok?," *Examiner*, November 14, 2010, http://www.examiner.com/article/the-Internet-vigilante-mob-justice-or-Internet-vigilantes-run-amok.

These early actions by Anonymous were important for the evolution of the group and its future direction. The tactics utilized in these early raids, virtual sit-ins, DDoS, and exfiltration, were reflective of not only the power of collective action but also the capability of the group's few skilled members. Yet all were part of Anonymous and up until that point, motivated mostly by the lulz. Quinn describes this period as Anonymous' inflection point and when the group realized the potential of collective action on the web and its ability to garner media attention.[344] According to one Anon (a member of Anonymous), these actions represented the group's instinctual drive towards "ultra-coordinated motherf[*]ckery [edited]."[345]

B. STRUCTURE

Despite the increasingly antagonistic and criminal nature of their actions, persons targeted by Anonymous had limited recourse since any response or reprisal was futile against a truly anonymous collective. Targeting an amorphous blob such as Anonymous was difficult at best since the members were unknown not only to the victim but also each other. This was evidenced by Turner's ineffective attempt to sue 4chan and other apparently unwitting virtual community hosts.

As an Internet based collective, Anonymous lacks organizational structure and leadership; however, more than makes up for this with its "unparalleled sense of democracy" and collaboration.[346] Inherent with most message boards and chat rooms is the ability and willingness to openly debate. Anonymous utilizes this platform to formulate ideas and action all the while respectful of the right to be heard. Not unlike the university campus of the 1960s or environmentalist journal publications, members of Anonymous, with the distinct advantage of anonymity, are able to speak their mind without fear of reprisal.

---

344 Norton, "Anonymous 101: Introduction to the Lulz."

345 Ibid.

346 "Why We Protest, Anonymous Activism Forum," Why We Protest, accessed July 24, 2014, http://whyweprotest.net/community/threads/project-chanology-a-new-chapter-in-social-movements.64296/.

According to Halupka, members of Anonymous also recognized the distinct advantage presented by this cloak of anonymity and were emboldened by the fact that "retaliation on an individualized basis (was) unfeasible, as a faceless mob, the target could only strike back at the collective identity of Anonymous rather than those who comprised it."[347] The role that anonymity played in the formation of Anonymous cannot be ignored since, during the nascent stages of other collectives such as SDS and Earth First!, protest actions required physical presence and witness making its members vulnerable to reprisal from authority and potentially its group members. Faced with this burden, overt actors are likely deterred from taking particular action for fear of reprisal or punishment. Once targeted by authority, groups like the Weathermen and ELF, went underground and formed autonomous cell structures designed to reduce their visibility. This presents a real and challenging problem for authority since anonymous collectives circumvent the underlying assumption of deterrence that the threat is both "definable and identifiable."[348] Anonymous and its hacker collective enjoy the technological benefit of anonymity from inception and at no cost to its members. However, because the identity of its members is unknown, Anonymous "cannot breed trust-based morality between individual members" but rather are forced to trust in the collective as a whole.[349] Nevertheless, the benefit of anonymity combined with the technological advantage of coordination provides Anonymous with the ability to quickly identify and attack targets with little or no warning.

C. DIRECT ACTION

Still unchallenged and becoming more recognizable on the international stage, Anons, beholden to the discourse on 4chan, were upset with Church of Scientology (CoS) efforts to remove a video of CoS member and actor Tom Cruise from YouTube, citing copyright infringement issues. Anonymous saw the CoS action as a direct assault on free speech and the Internet freedoms they hold in high regard. Hacktivists have long held that

---

347 Halupka, "The Evolution of Anonymous as a Political Actor," 41.

348 Iverson, *The Ring of Gyges*.

349 Rebecca Wright, "Hives, Damn Hives, and the Internet," *The Morningside Review*, July 11, 2014, http://morningsidereview.org/essay/hives-damn-hives-and-the-Internet/.

the Internet should be a free domain for speech and action. In 1999, a hacktivist group called Hacktivismo declared that "full respect for human rights and fundamental freedoms includes the liberty of fair and reasonable access to information, whether by shortwave radio, air mail, simple telephony, the global Internet, or other media."[350] According to Samuel, this view is widely held by politically motivated hackers who hold that online freedoms and freedom of speech are "core values of Internet culture."[351] This was no different for members if Anonymous, who after debating the actions of the CoS, self-appointed themselves as guardians of free speech on the web. According to one Anon:

> I think it's time for /b/ to do something big. People need to understand not to f*k with /b/, and talk about nothing for ten minutes, and expect people to give their money to an organization that makes absolutely no f*king sense. I'm talking about 'hacking' or 'taking down' the official Scientology website. It's time to use our resources to do something we believe is right. It's time to do something big again, /b/. Talk amongst one another, find a better place to plan it, and then carry out what can and must be done. It's time, /b/.[352]

Skeptical comments about such an attack or possibility of success soon evolved into increasing support as more members joined in the debate. On January 18, 2008, members of Anonymous once again banded together to conduct a series of attacks (dubbed Project Chanology) against the CoS that included such tactics as DDoS, prank calls, and overwhelming fax machines. Due to the open nature of 4chan and other message boards, skillful members of Anonymous were able to distribute their disruptive code or scripts to less skilled members who, because of their sheer number, were able to effectively overwhelm their targets, in this case, the CoS web servers. According to a *Los Angeles Times* article, Anonymous had roughly 9,000 members during the initiation

---

350 Elinor Mills, "Old-Time Hacktivists: Anonymous, You've Crossed the Line," Cnet, March 30, 2012, http://www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line/.

351 Samuel, "Hacktivism and the Future of Political Participation," 206.

352 Chris Landers, "Serious Business: Anonymous Takes on Scientology (and Isn't Afraid of Anything)," *Citypaper*, April 2, 2008, http://www2.citypaper.com/arts/story.asp?id=15543.

phase of Project Chanology.[353] Although DDoS attacks can effectively disrupt communication with the web, the actions by Anonymous more importantly garnered national media attention once again elevating awareness of the group and this time, attracting global support.

During the CoS raid, Anonymous set up a series of different channels designed to orchestrate and direct action. The channels were used to facilitate the group's recruitment efforts and helped to sustain the group's attack momentum by providing updates on the raid's continuing success with Anonymous press releases. One such channel, dubbed "#press," hosted a press release entitled "Internet Group Anonymous Declares War on Scientology."[354]

Along these same lines, on January 21, 2008, Anonymous posted a YouTube video, condemning the actions of CoS.[355] In less than one month, the video received approximately 2 million views revealing the remarkable prominence and reach of the group.[356] Utilizing the message boards and other social media sites, Anonymous called for physical protest actions resulting in "hundreds of thousands of demonstrators in nine hundred cities" around the world.[357] Showing solidarity with the online collective, many of the protestors wore Guy Fawkes masks[358] to conceal their physical identities and remain anonymous. The mask has since become synonymous with Anonymous.

Project Chanology not only placed Anonymous on an international platform, but it gave the group a purpose. By aligning with the causes of anti-censorship and free speech, Anonymous unwittingly garnered the attention and support of a terrestrial-base

---

353 Jim Puzzanghera, "Scientology Feud with Its Critics Takes to Internet," *LA Times*, February 5, 2005, http://www.latimes.com/local/la-me-scientology5feb05-story.html.

354 Parmy Olson, *We Are Anonymous* (New York: Little, Brown and Company, 2012), 71.

355 Patrick Barkham, "Hackers Declare War on Scientologists amid Claims of Heavy-Handed Cruise Control," *The Guardian*, February 3, 2008, http://www.theguardian.com/technology/2008/feb/04/news.

356 Brian Braiker, "'Anonymous' Takes on Scientology," *Newsweek*, March 13, 2010, http://www.newsweek.com/anonymous-takes-scientology-93883.

357 Christopher Alessi, "Why Is Occupy Wall Street Going Global?," *The Atlantic*, October 18, 2011, http://www.theatlantic.com/international/archive/2011/10/why-is-occupy-wall-street-going-global/246879/.

358 A mask referred to is a stylize depiction of the mask of Guy Fawkes, who was the most prominent member of the Gunpowder Plot, the 1605 attempt to blow up London's House of Lords. "Guy Hawkes Mask," *Wikipedia*, accessed September 18, 2014, http://en.wikipedia.org/wiki/Guy_Fawkes_mask.

willing to join forces with the Internet-based collective. By formulating a true identity, Anonymous, perhaps fortuitously, moved closer to becoming a social movement.

However, unlike terrestrial-based social movements, Anonymous did not fit the mold of social movement theory since it "lack(ed) the economic, cultural and structural components to succeed."[359] Since Anonymous has no discernible leadership, its actions result from the web-based discourse of its members. Through skillful use of the Internet, Anonymous has eliminated the need for structure and instead organizes itself via a "highly fluid system of networks and dynamic communication" capable of swarming via the web.[360] This was evidenced by the remarkable support for Project Chanology.

As previously discussed, the Internet, specifically social media, bridges the resource gap required by terrestrial based movements of people and money. Web-based collectives can quickly gather, debate, and take action with little or no warning capitalizing on the distinct advantage offered by the web. Samuel effectively argues that Anonymous and other hacktivist collectives represent a "new social movement" that poses a challenge to traditional social movement theory.[361] According to Samuel, scholars have "yet to confront a movement defined by its common method rather than its common purpose."[362] Anonymous is a group formed by discourse on the web, and it adopts ideological justifications for its actions. The efforts to restrict access to a YouTube video galvanized a generation of millennials who grew up on the web. Furthermore, Anonymous now has a recruitment base and a purpose.

D. FRACTURE

As an amorphous blob void of leadership, it is difficult to identify points of discourse within the group since actions are defined by the majority. The literature also provides little insight as to real identities of the group's members since the strength of Anonymous is derived from its anonymity. However, the successful raid against the CoS

359 "Why We Protest, Anonymous Activism Forum," Why We Protest.

360 Ibid.

361 Samuel, *Decoding Hacktivism: Purpose, Method, and Identity in a New Social Movement*.

362 Ibid.

increased notoriety from both the media and the general public making Anonymous much larger than just a group of hackers on the web. This increased following also piqued interest from cyber security firms and law enforcement both intent on disrupting the group's activities. One such firm's willingness to confront Anonymous altered the direction and focus of the hacktivist group.

Aaron Burr, CEO of HBGary Federal (HBG), a computer security firm, intrigued by the actions of Anonymous, joined the 4chan boards to monitor the activities of Anons and become more familiar with the group's identity.[363] Keeping tab, Burr believed he had enough information about the group and on February 5, 2011, in an article in the *Financial Times*, publicly announced that he had "compiled a dossier of their alleged real names."[364] Considering this as both a challenge and a threat, certain members of Anonymous banded together to undermine Burr's claims and orchestrate a direct raid attack against HBG and its employees.

The Anonymous message boards were busy with traffic and members from around the world banded together to discuss the article. Two such members, "Sabu" and "Topiary" (later identified via law enforcement efforts as Hector Monsegur and Jake Davis respectively), who were meeting online for the first time, were invited into a "locked" chat room session by another Anon known only as "Tflow," a skilled teenage programmer from the United Kingdom.[365] The locked sessions ensured that only invited persons were allowed into the discussion thus extricating the group from the larger collective. The group was also distinguished in that it contained only those members deemed to be skillful or committed to Anonymous as noted by previous contributions or tech savvy comments. This is significant because it reflects a nascent effort by a group of likeminded actors to extricate themselves from the larger collective to begin more

363 Olson, *We Are Anonymous*, 8.

364 Nate Anderson, "Anonymous vs. HBGary: The Aftermath," Ars Technica, February 25, 2011, http://arstechnica.com/tech-policy/2011/02/anonymous-vs-hbgary-the-aftermath/.

365 Olson, *We Are Anonymous*, 10.

focused and purposeful action. The new secure chat room was dubbed "#InternetFeds."[366]

Once isolated from the larger collective, the group initiated a series of actions against HBG that included an elevation from previous tactics. The Internet Feds conducted reconnaissance of HBG servers and identified a number of security flaws that, once exploited, offered them access to Aaron Burr's email, Twitter, and LinkedIn accounts as well as proprietary source code for HBG. The group defaced HBG's website and also extracted email data and source code, which was subsequently posted on pastebin.com, a popular plain text posting site used to store text online. The emails revealed HBG's sensitive relationship with the U.S. government and company efforts to solicit government contracts to discredit WikiLeaks and develop undetectable software code for the government.[367] The emails also revealed Burr's intention to meet with the FBI concerning his findings on Anonymous. Irreparably harmed by the Internet Feds, Aaron Burr stepped down as the company's Chief Executive Officer just a few weeks after the attacks.[368]

The group's willingness to intensify its actions is perhaps more indicative of the select collective's sophisticated skillset. However, the group's decision to act is also reflective of the challenge-response dynamic that suggests groups, in order to maintain their identity, must respond to threats or risk losing their acceptance. Increasingly aware of the threat posed by their actions, security firms such as HBG and law enforcement alike were motivated to identify and disrupt the hacktivist collective. The social identity theory suggests that Anonymous, now a globally recognized movement and/or brand, would be required to fight to remain the sentinel for free speech on the web. As an Internet-based group that values anonymity, recourse could only be carried out via disruptive web-based attacks. This meant that, once challenged, Anonymous or Internet

366 Ibid., 141.

367 Nate Anderson, "Black Ops: How HBGary Wrote Backdoors for the Government," Ars Technica, February 21, 2011, http://arstechnica.com/tech-policy/2011/02/black-ops-how-hbgary-wrote-backdoors-and-rootkits-for-the-government/.

368 Peter Bright, "With Arrests, HBGary Hack Saga Finally, Ends," Ars Technica, March 10, 2012, http://arstechnica.com/tech-policy/2012/03/the-hbgary-saga-nears-its-end/.

Feds, in order to maintain or improve its standing vis-a-vis the government and/or white hat security firms, used cyber attacks as a "public proclamation" to damage the credibility and status of its adversary.[369] The attack against HBG was an effective primary response with secondary effects against the U.S. government. Anonymous was no longer focused on the lulz.

During this same period in 2011, Internet Feds and other members of Anonymous were increasingly focused on global events, such as the Arab Spring and the Occupy movement.[370] The group supported these movements by orchestrating website defacements against the Tunisian government as well as working with other hacker collectives such as Telecomix to facilitate discrete online communication channels for Tunisian protesters.[371] Taking advantage of its now immense following, Anonymous, via a video on YouTube, effectively spread the word about a Canadian magazine's call to "occupy Wall Street" (a redress about social and economic inequality in the United States) enabling a localized movement to evolve into a global protest targeting financial institutions and other symbols of social inequality.[372] The existential efforts by Anonymous to support the terrestrial Occupy and Arab Spring movements expanded the group's scope and purpose now unbound by a single ideology or purpose.

The growing influence of Anonymous and the success of the Internet Feds efforts also brought more attention from police and anti-Anonymous security firms who increased their efforts to unmask the hackers. By trolling in the same chat rooms used by Anonymous, non-members, adept at social engineering (a significant trait of successful hackers) were able to collect chat logs from unwitting members of Anonymous that

---

369 Strindberg, "Social Identity Theory and the Study of Terrorism."

370 The Occupy Movement is a global protest movement originating in 2011 against social and economic inequality and was specifically focused on the perceived power of the financial industry. The Arab Spring was a 2011 large-scale revolutionary protest movement that targeted numerous unjust and corrupt governments in the Middle East resulting in the removal of some of the nation's long standing rulers.

371 Shyamantha Asokan, "The 'Hacktivists' of Telecomix Lend a Hand to the Arab Spring," *The Washington Post*, December 6, 2011, http://www.washingtonpost.com/lifestyle/style/the-hacktivists-of-telecomix-lend-a-hand-to-the-arab-spring/2011/12/05/gIQAAosraO_story.html.

372 Captain, "The Real Role Of Anonymous In Occupy Wall Street."

ultimately revealed the identities of some Anons including Sabu and Topiary.[373] Aware of their potential exposure and wanting to escape from the increased scrutiny, select members of Internet Feds, no longer able to trust the group's chat room communication channels, retreated to private communications on a web server owned by Sabu. The very platform used to create Anonymous had now grown too big to trust, a fear realized by the successful arrests and of dozens of people with suspected ties to Anonymous activities.[374]

It was in this private network that Sabu informed the smaller group about his previous exploits and began to assert his dominate personality. Described as a "principled warrior" whose rhetoric was "redolent of the most radical of sixties activists," Sabu's skills and strong personality elevated him to leadership status within the group.[375] Parmy Olson, author of *We Are Anonymous*, an expose of the hacktivist collective, describes Sabu as a real activist motivated by social and political change. According to Olson, Sabu's frequent run-ins with law enforcement made him "deeply resentful of people who abused positions of authority."[376] With a particular disposition towards white hat security firms and police corruption, Sabu was attracted to Anonymous because of its lack of hierarchy.[377] Cognizant of successful efforts by the FBI and law enforcement to penetrate hierarchical group structures, Sabu believed Anonymous' amorphous nature was resilient to law enforcement efforts against it. Now as a small cluster within the larger Anonymous collective, Sabu and select members believed they had effectively formed their safe haven. Sabu's role as leader within the group also provided purpose.

In May 2011, the group, now aligned with Sabu's slant, launched another Anonymous offshoot called LulzSec, short for Lulz Security. With a proclivity towards exposing security flaws in corporate, government, and law enforcement networks,

---

373 Olson, *We Are Anonymous*, 211–214.

374 Jana Winter, "16 Suspected 'Anonymous' Hackers Arrested in Nationwide Sweep," *Fox News*, July 19, 2011, http://www.foxnews.com/tech/2011/07/19/exclusive-fbi-search-warrants-nationwide-hunt-anonymous/.

375 Steve Fishman, "How LulzSec's Sabu Became the Most Influential Hacker in the World," *New York Magazine*, June 3, 2012, http://nymag.com/news/features/lulzsec-sabu-2012-6/index2.html.

376 Olson, *We Are Anonymous*, 233.

377 Ibid., 233–235.

LulzSec embarked on an indiscriminate 50-day campaign whose targets included a number of corporate, government and law enforcement agencies, including Fox Television, Sony Corps, the U.S. Senate, the Central Intelligence Agency, and police departments. A skilled collective, the group defaced websites and hacked/exfiltrated sensitive data and posted personal information and emails on public websites. A brazen Sabu exploited a security flaw in the public facing website for InfraGuard, a joint FBI and private sector information sharing partnership, and released personal information of its members. A *Wall Street Journal* article concerning the growing list of LulzSec victims stated, "Almost anyone is a target."[378]

In the midst of LulzSec's chaotic campaign, the FBI, with information received from a white hat security outfit called Backtrace, identified Sabu as 27-year old Hector Monsegur and, on June 7, 2011, arrested him at his apartment residence in a New York City housing project.[379] Court documents revealed that Monsegur cooperated with the FBI and quickly helped to identify "Topiary" as Jake Davis, a 17-year old from Shetland, England and "TFlow" as Mustafa Al-Bassam, a 16-year old male identified in England—both of whom were subsequently arrested by the United Kingdom's Metropolitan Police Department.[380]

Though effectively disrupting this Anonymous splinter group, LulzSec and in particular, Sabu, were representations of real activists purposely exploiting the Internet for political ideology. Sabu's radical expressions appeared based in part by his own perceived mistreatment and social injustice at the hands of authority. Much like the Days of Rage protests by the then nascent Weathermen, LulzSec's purposeful actions against security, law enforcement, and other representations of authority were efforts to legitimize Anonymous as a political actor in as much as it was an effort to right a perceived wrong.

---

[378] Ben Worthen et al., "Lockheed, PBS Join Roster of Hacking Victims," *The Wall Street Journal*, May 31, 2011, http://online.wsj.com/news/articles/SB10001424052702304563104576355623894502788.

[379] Fishman, "How LulzSec's Sabu Became the Most Influential Hacker in the World."

[380] Preet Bharara and James J. Pastore, Jr., United States of America v. Hector Xavier Monsegur, a/k/a "Sabu," United States District Court, Southern District of New York 2014.

However, LulzSec was not alone in its beliefs. Another Anon, known as "sup_g" by the online community, later identified as Jeremy Hammond by the FBI, was a Chicago native already deeply ingrained in the activist lifestyle. Described as an "electronic Robin Hood" by Chicago magazine, Hammond participated in a number of anti-capitalist demonstrations before Anonymous or the Occupy movements were household names.[381] A skilled hacker, Hammond, at 22 years of age, was arrested for hacking a conservative website and stealing 5,000 credit cards for the purpose of charging donations to "progressive causes."[382] During a 2008 interview by *Rolling Stone* magazine, Hammond described himself as an "anarchist-communist—as in I believe we need to abolish capitalism and the state in its entirety to realize a free egalitarian society."[383]

During a 2004 DefCon hacker convention in Las Vegas, Hammond gave a passionate speech about the virtues of electronic civil disobedience and the need for hackers to unite and disrupt the 2004 Republican National Convention by shutting the power down to Madison Square Garden, the host venue for the convention. During an interview with *Chicago* magazine, Hammond reiterated similar overtures stating "As hackers we can learn these systems, manipulate these systems, and shut down these systems if we need to."[384] Hammond would later recount that it was during this period that he began to conjure thoughts of an insurgency movement called the "Internet Liberation Front" much like the autonomous animal and environmental movements discussed in the previous chapter.[385] Later introduced to Bill Ayers, founder of the Weathermen, by a local leader of Chicago's Rainforest Action Network, Hammond questioned the idea of willingly getting arrested as an act of civil disobedience stating

---

381 Stuart Luman, "The Hacktivist," *Chicago*, June 25, 2007, http://www.chicagomag.com/Chicago-Magazine/July-2007/The-Hacktivist/.

382 Janet Reitman, "Jeremy Hammond: Rise and Fall of the Legendary Hacker," *Rolling Stone*, December 7, 2012, http://www.rollingstone.com/culture/news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-20121207?print=true.

383 Ibid.

384 Luman, "The Hacktivist."

385 Reitman, "Jeremy Hammond: Rise and Fall of the Legendary Hacker."

"The revolution to me is about not getting in their jails" and doubted the effectiveness of sit-ins and local petitions.[386]

Hammond's comments regarding activism are insightful as they portray genuine examples of the potential for hacktivism and initial attempts to create a truly disruptive collective. Hammond's calls to action, though unfulfilled, reveal his awareness and radical inclination towards hacktivism in the proper setting. Hammond's attraction to non-hierarchical structures, though reflective of anarchist ideology, also reflect a learned agent, possibly influenced by other radical groups such as the Weathermen and ELF. The Internet Liberation Front, though notional, represent Hammond's significant appreciation for the power of the Internet. Outside influences like Ayers would soon be replaced by web-based influences providing an advantageous venue for action.

Inspired by the surprising effectiveness of the December 2010 Anonymous attacks against PayPal, Visa, and MasterCard for their refusal to process donations for WikiLeaks, a web hosting site created by Julian Assange to publish classified U.S. government documents stolen by U.S. Army intelligence analyst Bradley Manning, Hammond joined Anonymous in chat room discussions and monitored those with whom he most closely aligned. Still the activist, Hammond participated in a number of physical Occupy protests actions and, discouraged by the repression of the movement, grew increasingly frustrated with the "limitations of peaceful protest, seeing it as reformist and ineffective."[387] However, as a hacktivist, Hammond joined Anonymous because, in his own words, "I believe in autonomous, decentralized direct actions."[388] Radically aligned with the anti-authoritative ideology of Sabu, LulzSec represented the new activist outlet Hammond had been looking for.

Already an admirer of LulzSec and the group's previous attacks against HBG, Hammond was contacted by Sabu during the summer of 2011 and accepted his invite to join LulzSec in a new Anonymous campaign called Antisec, a self-proclaimed effort to

386 Ibid.

387 "Jeremy Hammond's Sentencing Statement," The Sparrow Project, November 15, 2013, http://www.sparrowmedia.net/2013/11/jeremy-hammond-sentence/.

388 Ibid.

steal and leak any classified government information and continue to target banks and other high ranking establishments.[389] Regardless of direction, the conjoining of Monsegur and Hammond, two highly skilled and unidentified hacktivists, represented the potential for likeminded hacktivists to form a more radical cluster for direct action. Hammond was all too willing and able to participate in Antisec and at the alleged direction of Sabu, he and other members of Anonymous embarked on a significant hacking campaign that cost corporations and banks hundreds of millions of dollars and also resulted in exfiltrating and leaking of large volumes of sensitive data obtained from security firms and U.S. government agencies.[390]

Under the direction of Sabu, Hammond hacked and exfiltrated large volumes of sensitive data from Stratfor, a geopolitical intelligence firm with strong ties to the U.S. government. Once obtained, Hammond posted over 50,000 pieces of credit card data he used to fraudulently process over $1 million in charitable donations, and he also released over 5 million emails that contained sensitive Stratfor relationships with corporate and government networks.[391] Hammond was arrested by the FBI on March 5, 2012.

With the help of Sabu, law enforcement identified a number of LulzSec and Anonymous members effectively putting an end to the Antisec campaign. Many of the hackers have pleaded guilty in exchange for lesser sentences; however, Hammond received a maximum 10 year sentence for his actions. Yet despite their arrests, Anonymous still lives on with many operations targeting websites of U.S. and foreign governments, corporations, and a number of their targets perceived as threats to social equality or free speech. Anons still supported the global Occupy movement and proceeded to hack the websites of government agencies and banking corporations. In September 2013, Anonymous resurfaced by hacking and leaking over one million Apple

---

389 Olson, *We Are Anonymous*, 332.

390 Cassell Bryan-Low and Siobhan Gorman, "Inside the Anonymous Army of 'Hacktivist' Attackers," *Wall Street Journal*, June 23, 2011, http://online.wsj.com/news/articles/SB10001424052702304887904576399871831156018.

391 Sean Gallagher, "Inside the Hacking of Stratfor: The FBI's Case against Antisec Member Anarchaos," Arstechnica, March 6, 2012, http://arstechnica.com/tech-policy/2012/03/inside-the-hacking-of-stratfor-the-fbis-case-against-antisec-member-anarchaos/.

user IDs allegedly stolen from an FBI laptop (a fact later refuted by the FBI.)[392] In an official pastebin statement, the group paid homage to Hammond labeling him as an "ideological motivated political dissident."[393] Though considered tame when compared to the period of time between Project Chanology and Antisec, Anonymous continues to remain a reactive body with the potential to strike anyone at any time.

In his final tweet as Topiary, Jake Davis, just prior to his arrest in the United Kingdom, stated "You cannot arrest an idea."[394] Despite the physical arrests of previous Anons, Norton asserts "Anonymous is beginning to plot a course without them, doubling down on its political mission."[395] Speaking truth to power and closely aligned to the ideology of Jeremy Hammond, an Anon identified as "CC3" has claimed that today the group is focusing "less on defacement and more on quietly taking over infrastructure" adding "the FBI doesn't have a clue about what we're doing which is good."[396]

E. CONCLUSION

Anonymous is the epitome of discourse in action for it was born from it. As an unwitting emergence from open web-based communication platforms, communicative discourse amongst tech savvy individuals evolved into a collection of likeminded collectives primarily interested in pranks and lulz. However, the power of the social media platforms such as 4chan fortuitously formed a collective void of purpose. Joined by the Internet, anonymous individuals engaged each other online formulating discussion and opinion that ultimately evolved into mischief and harassment. Joined only by the Internet, Anonymous originally lacked purpose and remained unaware of the authoritative power afforded by 4chan and similar web-based platforms. However, the

392 Parmy Olson, "FBI Agent's Laptop 'Hacked' To Grab 12 Million Apple IDs—UPDATED," *Forbes*, September 4, 2012, http://www.forbes.com/sites/parmyolson/2012/09/04/fbi-agents-laptop-hacked-to-grab-12-million-apple-ids-anonymous-claims/.

393 "Special #FFF Edition—Anonymous," Pastebin.com, September 3, 2012, http://pastebin.com/nfVT7b0Z

394 Olson, *We Are Anonymous*, 406.

395 Quinn Norton "How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down," *Wired*, July 3, 2012, http://www.wired.com/2012/07/ff_anonymous/all/.

396 Reitman, "Jeremy Hammond: Rise and Fall of the Legendary Hacker."

anonymity afforded by 4chan and other relay channels as well as the large number of participants on the boards resulted in dynamic causes like corruption to be replaced by a "dynamic market of causes."[397] However, as revealed by the open structure of SDS, playing host to a dynamic market of causes is not necessarily advantageous. In 4chan, the high levels of membership also brought with it a number of diverse narratives that made it difficult for action. Therefore, with little or no cost to its members, these open communities formed smaller clusters around identities formed by rhetoric and action.

Anonymous' non-hierarchical structure is loosely connected by the ideals formulated in web-based chat room such as 4chan. As an Internet based collective, Anonymous was born from its unparalleled sense of democracy and collaboration that enabled all members to participate and guide the message. Constant discourse and debate shaped daily action and at times elevates more influential members to take lead on the issue of the day. Unguided by a single purpose or ideology, Anons have been reactive and swarming around a cause only to return to 4chan and other boards failing to coalesce into lasting or sustained action. These loose ties or bonds have negative impact on unity and coordination making it difficult to form lasting coalitions.[398] However, since Anonymous is a reactive body, its threat is always imminent.

The lack of direction, purpose, and trust, ultimately led to the formation of smaller cells of hacktivists, such as the InternetFeds who, doubting the majority's ability to force change, opted to form a more active coalition towards direct action. As a decentralized group of activist cells populating a number of different message boards, Anonymous began operating in a more secure environment. The independence afforded by this new environment allows for intimacy, flexibility, and adaptiveness that made infiltration difficult.[399] As one of the most skilled and politically motivated members of his cell, Sabu assumed a leadership position of Internet Feds. According to Topiary, the group did not want to be constrained by the larger collective and its basic principles for targeting,

397 Rid, *Cyber War Will Not Take Place*, 123.

398 Ibid., 123.

399 Halupka, "The Evolution of Anonymous as a Political Actor," 26.

which focused on the ideals of free expression.[400] For the hacktivist collective within Anonymous, this decentralized structure served to free Sabu and others from the ideological restraint of the majority and enabled them to pursue their own interpretative action.

According to Biesecker-Mast, "confrontation" is a place "between meaning and antagonism, between hegemony and subversion, and between a movement's promise and its inherent limits."[401] For hacktivists, the online collective is both its promise and its demise for the global reach of its communicative platform is also the source for eternal discourse. Competing with the dynamic market of ideas forms the basis for internal conflict that, when confronted by oppression, may force more deeply committed members to use force.

[400] Olson, *We Are Anonymous*, 244.

[401] Gerald J. Biesecker-Mast, "How To Read Social Movement Rhetorics as Discursive Events," 1996, http://www.bluffton.edu/~mastg/social.htm.

THIS PAGE LEFT INTENTIONALLY LEFT BLANK

VIII. FINDINGS AND CONCLUSION

A. INTRODUCTION

A limited amount of research had been conducted on the significance of the Internet as a platform for activism and the role of venue in the furtherance of social movements. Although a number of studies have been conducted on social movements and the praxis behind such movements, little research existed as to whether web-based social movements were significantly advantaged and thus a particular threat to homeland security interests. Until recently, hacktivism has been an accepted form of civil disobedience since it is accepted as a non-violent act of protest; however, the Internet as venue for disruption remain separated in the context of hacktivist research. This thesis has focused on whether the Internet and the availability of increasingly sophisticated web-based technologies provides activists a significant advantage compared to terrestrial-based movements. In ascertaining whether hacktivist movements present a risk to homeland security, it is important to understand the potential advantage that the Internet provides.

B. FINDINGS

The sustainability of the SDS and Earth First! movements was in part attributable to the galvanizing issues they each represented as well as the structure that each group utilized for action. Once adopted, the issue becomes the motivator for the group and, in decentralized networks, easily enacted by the multitude of supporters within the cell structures. For SDS, the campus venue enabled collective action that for a while was met with only limited authoritative action. However, as the group became more popular and more engaged in direct action, repressive authoritative actions limited the movement's ability to formulate change. Unequipped to confront the government's security apparatus, the resolve of SDS's followers weakened enabling more influential members to redirect the group's platform, which resulted in increased discourse and debate.

Likewise for Earth First! that, after a series of direct protest actions against corporate entities within the logging industry, also found itself engaged with a much

stronger authoritative agent capable of limiting the group's actions. Unwilling to confront authority with violence, founder Foreman's mainstream policies isolated more extreme members who believed that increasingly violent action was necessary to force change in environmental policy. However, the lack of direct control over decentralized networks lessened Foreman's ability to control the group's actions. Extreme Earth First! members formed more violent cell structures and allied with ELF. Thus, the life cycle of the social movements appears directly attributable to authoritative challenge and resulting discourse. Though galvanized, the single-issue groups failed to create change resulting in its demise and ultimate fracture.

The life cycle of the terrestrial-based movement depicted in Figure 2 diagram is in part influenced by the findings of Armand Mauss in his 1975 book *Social Problems as Social Movements*.[402] The development of SDS and Earth First! from mostly singular issues or ideologies that galvanized a targeted populace that when challenged, waned and became susceptible to discourse. Both SDS and Earth First! thus became most vulnerable at its height since the popularity and success of its growth and movement helped to draw many who were not directly aligned with its focus. Ironically, the successful growth of the movement is what also lead to its demise. Larger collectives also attract diverse members and the attention of authority potentially diluting its strength. The larger collective mediates itself leading to purposeful and mainstream actions. SDS's use of mostly passive tactics, though successful at drawing media and public attention, were ineffective at forcing policy change. Efforts to move such bodies towards more radical action are ineffective as noted by the less popular and ineffective Day of Rage protests. Earth First!'s inability to curb perceived harmful environmental polices forced extremists to break away from the mainstream and formulate their own direct action network.

In single issues groups, failure to create change not only leads to a group's demise, but it can also force the fracture necessary for more isolated and extreme, members to create violent action groups. Already predisposed, the more extreme groups

---

402 Armand L. Mauss, "The Genesis of Social Problem-Movements," in *Social Problems as Social Movements*, ed. Armand L. Mauss, 38–71 (Philadelphia: J.B. Lippincott, Co., 1975), http://media.pfeiffer.edu/lridener/courses/spassm.html.

return to a pattern of direct action able and willing to confront authority. The cycle repeats itself until its resources are no longer able to support the movement. Continually challenged by authority, the Weathermen were forced to remain underground and eventually disrupted by law enforcement and a largely ineffective campaign of violence. However, unlike the Weathermen, ELF's leaderless resistance movement of decentralized cell structures persists to this day in a somewhat formidable role for the environmental movement.

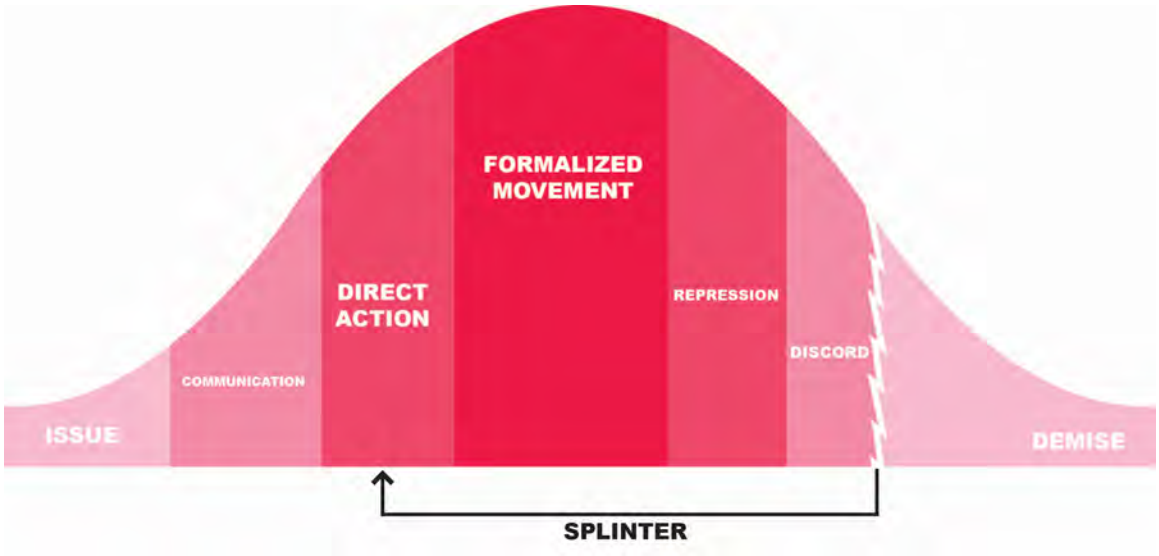

Figure 2. Life Cycle of Traditional Social Movement

As web-based movements, groups like Anonymous derive the benefit of collective action from outset as hacktivists react to issues brought forth from collective web-based discourse. Issues are crowd sourced creating hacktivist actions that are both reactive and unpredictable. Thus, hacktivist groups originate further along the curve since they are spawned from the collective (see Figure 3).

Since web-based actions are difficult to defend against, hacktivists formulate quick action that, depending upon their intent, may either be quick and decisive or sustain for a period of time. Anonymous, like SDS and Earth First! is a self-regulatory body that often results in mainstream action. Their protest tactics, though disruptive, rarely force change but rather elevate issues for greater public awareness. However, groups like

LulzSec are also reflective of extremists within the organization that are dissatisfied with mainstream arguments and splinter to formulate more disruptive action on behalf of the collective. These splinter groups, unwilling to accept mainstream thought or repression from authority, utilize their advantageous platform to engage in a repetitive cycle of direct action that may be focused or broad depending upon the issue. The actions by LulzSec were indiscriminate and targeted a number of private and corporate sector entities. The cycle ended when law enforcement arrested a number of the group's key members.

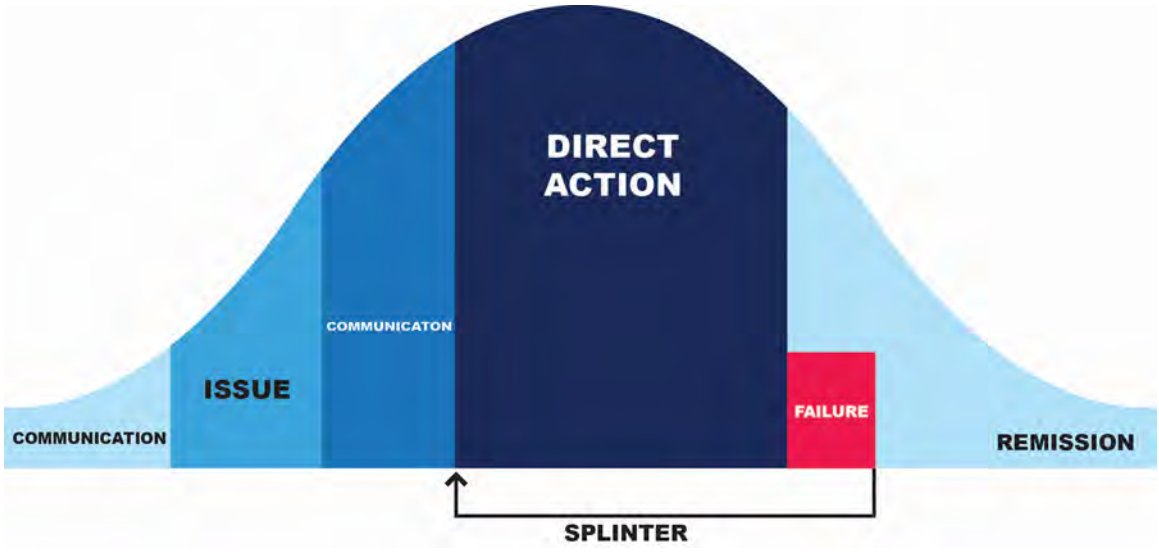

Figure 3. Life Cycle of Single Hacktivist Action

The difference with hacktivism is that when repressed by authority, the process continues since the operating venue is the Internet, which offers an endless and technically savvy resource. Unlike single issue groups, Anonymous is spawned from a multitude of ideas that continuously spawns discourse and action (see Figure 4).

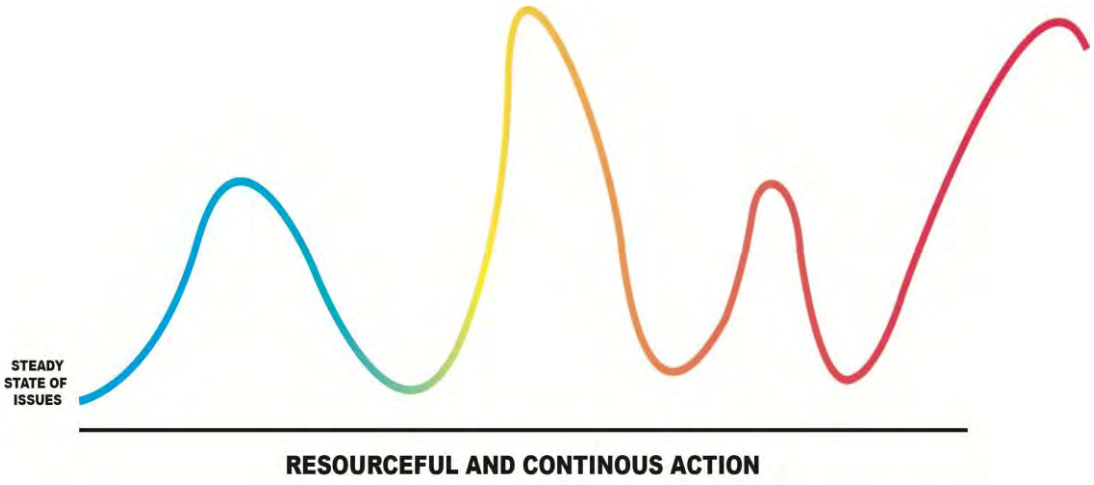

Figure 4. Internet as Source for Continuous Action

In addition to the life cycle distinctions between web-based and terrestrial-based social movements, a number of other findings offer insight as to the distinct and concerning advantage enjoyed by web-based activists.

1. *The Internet as venue provides a unique advantage for hacktivists to mobilize and generate action; however, the sustenance for these actions is potentially undermined by the weak ties inherent to web based relations.*

Venue plays a specific role not only in the origin of the social movement but also the resource mobilization requirements necessary for a movement to take hold. A movement succeeds when it is able to mobilize and produce a level of response that influences policy and/or exerts political pressure on the state. Social movements rely upon money, resources, and labor for success. The SDS achieved limited success via the campus movement; however, the group was unable to garner support in neighboring communities and thus had limited mobility beyond the campus venue. Hacktivists have immediate access to global resource via social media and, with no monetary or social cost, can effectively identify likeminded individuals. The ability to quickly galvanize and garner support for any number of causes is a unique advantage provided by social media that provides a new global generation a real and genuine solution for the right to be heard.

Absent censorship, the Internet provides unique communication, organization, and mobilization advantages over traditional venues, such as campuses and localized meetings, enabling forum participants to seek similar interests within the larger collective. However, this unique advantage appears to be offset by the weak ties formulated via social media as evidenced by the quick dissolution of LulzSec, which makes the hacktivist's goal for policy change more difficult. In contrary, the bonds formulated by members of SDS and Earth First! in more intimate venues sustained for long periods of time even when confronted by authority.

2. *The Internet provides immediate structural and security advantages for the formation of web-based social movements.*

The Weathermen, Earth First!, and its North American splinter group ELF, all adopted decentralized networks to achieve their goals of not only direct action but sustainability. When faced with repeated challenges from authority, the groups decentralized to create safe havens that not only increased their chance for survival but also helped to strengthen their resolve for direct action. Reflecting their confidence in decentralized networks, the Weathermen announced their intent to go underground. Hacktivists by definition already exist in a non-hierarchical, web-based environment that provides the necessary tools for a web based safe haven of anonymity.

Social media platforms permit participants to debate more freely than traditional venues without fear of recourse and over time formulating ideological clusters in a new decentralized layer. Hacktivist groups such as Anonymous are proficient at using the Internet to formulate debates around a number of issues allowing discourse to dictate their actions. However, as a "dynamic market of causes," the forum debates rarely result in action as the number of participants and issues dilute the majority.[403] Security risks are posed by smaller collectives of more radically aligned hacktivists who, by the very nature of the Internet, can cause significant disruption. Formed from flat organizations, these new self-directed clusters can easily identify and isolate more skilled or radical members from across the globe to create a new movement. Thus, large collectives like

403 Rid, *Cyber War Will Not Take Place*, 123.

Anonymous, as a self-policing body, lose the elements of control and influence offered by the majority.

3. *Web-based anonymity provides a multifaceted and qualitative advantage that can be exploited by an adversary.*

As a collective born of the Internet, hacktivists have already gained the distinct advantage of anonymity as evidenced by web-based anonymization tools. However, these physical tools are overshadowed by the psychological effects of anonymity derived within larger collectives. As postulated by Chang, the effect anonymity has on producing uninhibited behavior is dependent upon group size; "the larger the size of the group, the higher the degree of anonymity experienced by the group's members."[404] Social media provides a unique platform for larger masses to gather anonymously, which increases susceptibility and risk for antisocial behavior. Thus, the social media platform provides immediate return for more radical members of web-based collectives, who, unlike their terrestrial based colleagues, utilize little effort to achieve this benefit. The repeated success of DDoS attacks against corporate and government sectors are successful representations of otherwise unwitting participants in criminal activity. Unlike terrestrial-based movements, which accept a level of risk when performing direct action, hacktivists, under the cloak of anonymity, can carry out attacks with little or no personal risk.

4. *Web-based anonymity provides a multifaceted and qualitative advantage that can be exploited by authority.*

The great irony in building anonymous collectives is that the true identity of the participants is unknown. Trust is developed overtime; however, unless the ties between participants are strong (an unlikely outcome of social media participants), large and small collectives are vulnerable to penetration. According to Lewicki and Tomlinson, the need for trust "arises from our interdependence with others" since it is necessary to "depend on other people to help us obtain, or at least not to frustrate, the outcomes we value."[405]

---

404 Chang. "The Role of Anonymity in Deindividuated Behavior."

405 Roy Lewicki and Edward Tomlinson, "Trust and Trust Building," Beyond Intractability 2003, http://www.beyondintractability.org/essay/trust-building.

However, this interdependence provides an element of risk since trust requires members to accept vulnerability based upon positive expectations of the intentions of another.[406] Investigators, using the same anonymization tools, exploit this trust and lurk inside the same hacktivists chat rooms and identify more radical or criminal elements for further investigation. Hammond and others within Anonymous, forced to rely on a level of blind trust, were victimized by the very anonymity they sought themselves.

5. *The Internet provides hacktivists a disproportionate platform for disruption.*

According to the FBI, since 1979, environmental and animal rights extremists in the United States are responsible for more than 2,000 crimes and over $110 million in economic loss.[407] However, this pales in comparison to the damage already caused by hacktivists. In 2010, hacktivists, utilizing basic DDoS and hacking skills carried out a single series of attacks against Sony Corporation that resulted in an estimated loss of $173 million.[408] Today, hacktivists can gain access to a number of sophisticated cyber weapons that, if utilized, can cause real and significant harm to America's critical infrastructure. Yet as a web based social movement, the current and potential threat posed by hacktivists remains underestimated. Up until LulzSec, hacktivists have been portrayed in generally positive light by global media; after all, no one has died from hacktivism. As hacktivist actions become more of the norm, the public will become desensitized and less aware of their actions.

However, rather than quell the hacktivist's motivation, hacktivists may increase their level of engagement to retain their prominence. According to Jenkins, terrorists want a lot of people watching, not a lot of people dead; however, he has also acknowledged that some terrorist, like al-Qaida, want a lot of people watching and

406 Ibid.

407 "FBI—Using Intel Against Eco-Terrorists," FBI, June 30, 2008, http://www.fbi.gov/news/stories/2008/june/ecoterror_063008.

408 Vamosi, "How Hacktivism Affects Us All."

dead.[409] If true, then more radical or ideological elements of a hacktivist movement are currently operating below their capacity since with little effort, they can equate the Internet's equivalent for both goals.

6. *Hacktivists Are Reactive Bodies Thus, Difficult to Defend Against*

Anonymous reacts to any number of emerging issues; this makes tracking or defending against their actions difficult. Likewise, authoritative response to hacktivism has been reactive as well. Hacktivists are confronted subsequent to their actions, usually after potentially devastating losses or disruption to corporate, government, or private sectors in America. Efforts to defend against hacktivism will not likely solve the problem since, as a global phenomenon, localized law enforcement efforts are unlikely to resolve the issues that hacktivists are motivated to address. The Anonymous raid against Sony Corporation in 2010 and subsequent raid by InternetFeds against HBGary Federal exemplifies both the reactive and resilient characteristics of hacktivist actions. These actions also symbolize the strategic challenges of defending against hacktivism since hacktivist decisions and actions are unpredictable. This is concerning since, as noted by Daniel Hepworth, professor of Criminal Justice at Murray State University, not all decisions are made rationally, especially when made by those who are reactive and/or emotionally compromised.[410]

C. CONCLUSION

This thesis displayed the multifaceted functions that the Internet can play in advancing social movement or hacktivism on the web. It demonstrated the inherent weakness in the Internet's architecture and how such open protocols have been coopted by threat actors for criminal and disruptive means. The easy availability of cyber based weapons have been used by hacktivists to cause millions of dollars in damage to

---

[409] Brian Michael Jenkins, "The New Age of Terrorism," in *The McGraw-Hill Homeland Security Handbook*, ed. David Kamien (New York: Mc-Graw Hill Companies, 2006), http://www.prgs.edu/content/dam/rand/pubs/reprints/2006/RAND_RP1215.pdf, 118.

[410] Daniel P. Hepworth, "Analysis of Al-Qaeda Terrorist Attacks to Investigate Rational Action," *Perspectives on Terrorism* 8, no. 3 (June 2014): 23–38, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/253/html.

government, private and commercial sector companies and organizations who are currently disadvantaged in defending against the nature of the hacktivists threat. Purposeful use of these weapons has already caused significant harm to critical infrastructure in nations like Iran, Estonia, and the U.S.; however, hacktivists have yet to join the fray. Hacktivist groups like Anonymous are socially unable to formulate disruptive action beyond the surface of DDoS and web defacement since the collective is mostly unskilled and open ended to a number of issues that dilute their debate. Discourse and debate is their purpose as it increases awareness and identifies those issues with a need for action. As was the case with SDS and Earth First!, harmful acts defeat the movement's purpose thus requiring restraint if it is to maintain the support of its majority.

Projecting the course of hacktivism is difficult; however, this thesis has shown that social movements, regardless of venue, have the praxis to evolve and splinter into more radical groups. Purposeful actions are carried out by minority members who formulate their own clusters based upon ideology and competence. For hacktivists, the Internet accelerates the process of collective identity. The threat is realized from resulting small clusters that splinter from the majority in order to sustain a secure operating environment and endorse more forceful action. Resulting law enforcement actions against these groups do not necessarily reflect failure of the movement since, as noted by Christina Foust assistant professor of communication studies at the University of Denver, such repressive effects "are felt as a reclamation of agency and autonomy in the present, as well as the future."[411] Thus, the transgressive clusters within Anonymous and other activist movements have ability to inspire future action.[412] The provocative comments of Anons subsequent to the arrests of Hammond and other members of LulzSec suggest a natural evolution of the web based social movement. Anonymous and other Internet-based movements have a never-ending pool of resource. To successfully control them will require even greater resource, suggesting, "hacktivism cannot be stopped any more

411 Foust, *Transgression as a Mode of Resistance*, 187.

412 Ibid.

than activism can."[413] The vulnerability of the Internet, availability of cyber based weapons, and threat of imminent action signals a hacktivist threat that is very real.

413 Colesky and Niekerk, *Hacktivism: Controlling the Effects*, 12.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abbey, Edward. *The Monkey Wrench Gang*. New York: Dream Garden Press, 1985.

Ablon, Lillian, Martin Libicki, and Andrea Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, RAND Corporation, 2014.

Advanced Persistent Threats (APTs). Atlanta, GA: Damballa, 2010. https://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf.

Alessi, Christopher. "Why Is Occupy Wall Street Going Global?" *The Atlantic*, October 18, 2011. http://www.theatlantic.com/international/archive/2011/10/why-is-occupy-wall-street-going-global/246879/.

Alexander, David. "Theft of F-35 Design Data Is Helping U.S. Adversaries." Reuters, June 19, 2013. http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619.

Anderson, Kent. *Hacktivism and Politically Motivated Computer Crime*. Encurve LLC. 2008. http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

Andrews, Suzanna, Bryan Burrough, and Sarah Ellison. "Snowden Speaks: A Vanity Fair Special Report." *Vanity Fair*. May 2014. http://www.vanityfair.com/politics/2014/05/edward-snowden-politics-interview.

Asbley, Karin, Bill Ayers, Bernadine Dohrn, John Jacobs, Jeff Jones, Gerry Long, Home Machtinger, Jim Mellen, Terry Robbins, Mark Rudd, and Steve Tappis. "You Don't Need a Weatherman to Know Which Way the Wind Blows." June 18, 1969. https://archive.org/details/YouDontNeedAWeathermanToKnowWhichWayTheWindBlows.

Asokan, Shyamantha. "The 'Hacktivists' of Telecomix Lend a Hand to the Arab Spring." *The Washington Post*, December 6, 2011. http://www.washingtonpost.com/lifestyle/style/the-hacktivists-of-telecomix-lend-a-hand-to-the-arab-spring/2011/12/05/gIQAAosraO_story.html.

Ault, Brian. "Joining the Nazi Party before 1930: Material Interests or Identity Politics?" In *Social Science History*, 26, no. 2. (2002): 273–310. http://muse.jhu.edu/journals/social_science_history/v026/26.2ault.pdf.

Bailey, Geoff. "The Making of a New Left: The Rise and Fall of SDS." *International Socialist Review*, October 2003. http://www.isreview.org/issues/31/sds.shtml.

Barkham, Patrick. "Hackers Declare War on Scientologists amid Claims of Heavy-Handed Cruise Control." *The Guardian*, February 3, 2008. http://www.theguardian.com/technology/2008/feb/04/news.

Berger, Peter L. and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Garden City, NY: Anchor Books, 1967.

Braiker, Brian. "'Anonymous' Takes on Scientology." *Newsweek*, March 13, 2010. http://www.newsweek.com/anonymous-takes-scientology-93883.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, and Steve Chon. "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime." *International Journal of Cyber Criminology* 8, no. 1 (2014). http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf.

Brodock, Katherine, Mary Joyce, and Timo Zaeck. *R@D 4—Digital Activism Survey Report 2009*. July 14, 2009. http://www.slideshare.net/DigiActive/rd-4-digital-activism-survey-report-2009.

Bruinsma, Gerben and Wim Bernasco. "Criminal Groups and Transnational Illegal Markets." *Crime, Law and Social Change* 41, no. 1 (2004): 79–94.

Bryan-Low, Cassell and Siobhan Gorman. "Inside the Anonymous Army of 'Hacktivist' Attackers." *Wall Street Journal*, June 23, 2011. http://online.wsj.com/news/articles/SB10001424052702304887904576399871831156018.

CBS News. "Cyberattack on Anti-Spam Group Spamhaus Has Ripple Effects." March 27, 2013. http://www.cbsnews.com/news/cyberattack-on-anti-spam-group-spamhaus-has-ripple-effects/.

Caldwell, Dan and Robert E. Williams, Jr. *Seeking Security in an Insecure World*. New York, New York: Rowman & Littlefield Publishers, 2006.

Chapman, Roger. *Culture Wars: An Encyclopedia of Issues, Viewpoints, and Voices*. Armonk, New York: M.E. Sharpe, 2009.

Chang, Jenna. "The Role of Anonymity in Deindividuated Behavior: A Comparison of Deindividuation Theory and the Social Identity Model of Deindividuation Effects (SIDE)." *The Pulse* 6, no. 1 (2008): 1–2. http://www.baylor.edu/content/services/document.php?id=77099

Clemente, Dave. *Cyber Security and Global Interdependence: What Is Critical?* London, United Kingdom: Chatham House, 2013. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf.

Coleman, Gabriella. "Our Weirdness Is Free." Accessed January 8, 2014. http://canopycanopycanopy.com/issues/15/contents/our_weirdness_is_free.

Colesky, Michael and Johan Van Niekerk. *Hacktivism: Controlling the Effects*. Port Elizabeth, South Africa: Nelson Mandela Metropolitan University. http://www.academia.edu/2033252/Hacktivism_-_Controlling_The_Effects

Cooper, Marilyn. "Environmental Rhetoric in the Age of Hegemonic Politics: Earth First! And the Nature Conservancy." In *Green Culture: Environmental Rhetoric in Contemporary America*, edited by Carl G. Herndl and Stuart C. Brown, 236–260. Madison, WI: University of Wisconsin Press, 1996.

Corbett, Edward P. J. "The Changing Strategies of Argumentation from Ancient to Modern Times." In *Practical Reasoning in Human Affairs: Studies in Honour of Chaim Perelman*, edited by James L. Golden and Joseph J. Pilotta, 21–36. 1st ed. Dordrecht, Netherlands: Springer, 1986.

Covill, Christopher J. *Greenpeace, Earth First! And The Earth Liberation Front: The Progression of the Radical Environmental Movement in America*. Kingston, RI: University of Rhode Island, 2008. http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1095&context=srhonorsprog

Deibert, Ronald and Rafal Rohozinski. "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet." In *Access Denied: The Practice and Policy of Global Internet Filtering*, edited by Ronald Diebert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, 123–49. Cambridge, MA: MIT Press, 2008.

Delio, Michelle. "Hacktivism and How It Got Here." *Wired*, July 14, 2004. http://www.wired.com/techbiz/it/news/2004/07/64193?currentPage=all

Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 239–288. Santa Monica, CA: RAND, 2001.

———. "Cyber Conflict as an Emergent Social Phenomenon." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hershey, PA: Information Science Reference, 2011. http://faculty.nps.edu/dedennin/publications/CyberConflict-EmergentSocialPhenomenon-final.pdf.

Dittman, Melissa. "What Makes Good People Do Bad Things?." *Monitor* 35, no. 9 (2004). http://www.apa.org/monitor/oct04/goodbad.aspx

Dreyfuss, Suelette. *Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier*. Sydney, Australia: Random House Australia 1997.

Edwards, Dana. "The Internet Vigilante Mob, Justice or Internet Vigilantes Run Amok?" *Examiner*, November 14, 2010. http://www.examiner.com/article/the-Internet-vigilante-mob-justice-or-Internet-vigilantes-run-amok

Ensor, David. "Al Qaeda Letter Called 'Chilling,'" *CNN*. October 12, 2005. http://www.cnn.com/2005/WORLD/meast/10/11/alqaeda.letter/.

Erving Goffman. *Frame Analysis: An Essay on the Organization of Experience*. Boston, MA: Northeastern University Press, 1986. http://is.muni.cz/el/1423/podzim2013/SOC571E/um/E.Goffman-FrameAnalysis.pdf.

Eyerman, Ron and Jamison, Andrew. *Social Movements: A Cognitive Approach*. University Park, PA: The Pennsylvania State University Press, 1991.

"FBI: Eco-Terrorism Remains No. 1 Domestic Terror Threat." *Fox News*, March 31, 2008. http://www.foxnews.com/story/2008/03/31/fbi-eco-terrorism-remains-no-1-domestic-terror-threat/.

Finn, Peter. "Cyber Assaults on Estonia Typify a New Battle Tactic." *The Washington Post*, May 19, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

Fisher, Marc. "In Tunisia, Act of One Fruit Vendor Sparks Wave of Revolution through Arab World." *The Washington Post*, March 26, 2011. http://www.washingtonpost.com/world/in-tunisia-act-of-one-fruit-vendor-sparks-wave-of-revolution-through-arab-world/2011/03/16/AFjfsueB_story.html.

Fishman, Steve. "How LulzSec's Sabu Became the Most Influential Hacker in the World." *New York Magazine*, June 3, 2012. http://nymag.com/news/features/lulzsec-sabu-2012-6/index2.html.

Fleming, Andrew. "Adbusters Sparks Wall Street Protest." *Vancouver Courier*, September 27, 2011. http://www.vancourier.com/news/adbusters-sparks-wall-street-protest-1.374299.

Foreman, Dave and Haywood, Bill. *Ecodefense: A Field Guide to Monkeywrenching*. 3rd ed. Ann Arbor, MI: Abbzug Press, 1993.

Foust, Christina R. *Transgression as a Mode of Resistance: Rethinking Social Movement in an Era of Corporate Globalization*. United Kingdom: Lexington Books, 2010.

Fuller, Abigail A. *The Structure and Process of Peace Movement Organizations: Effects on Participation*. Boulder: University of Colorado, 1989.

Gerlach, Luther P. "The Structure of Social Components: Environmental Activism and Its Opponents." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and John Rondfelt. Santa Monica, California: RAND, 2001.

Gladwell, Malcolm. "Small Change." *The New Yorker*, October 4, 2010. http://www.newyorker.com/magazine/2010/10/04/small-change-3?currentPage=all.

Glater, Jonathan D. "Privacy for People Who Don't Show Their Navels." *New York Times*, January 25, 2006. http://www.nytimes.com/2006/01/25/technology/techspecial2/25privacy.html?_r=0.

Goffman, Erving. *Frame Analysis: An Essay on the Organization of Experience*. Boston, MA: Northeastern University Press, 1986. http://is.muni.cz/el/1423/podzim2013/SOC571E/um/E.Goffman-FrameAnalysis.pdf.

Goins, Christopher and Pete Winn. "Chinese Hackers Stole Plans for America's New Joint Strike Fighter Plane, Says Investigations Subcommittee Chair." *CNS News*, April 25, 2012. http://cnsnews.com/news/article/chinese-hackers-stole-plans-americas-new-joint-strike-fighter-plane-says-investigations.

Goldstein, Joshua. *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution*. Cambridge, MA: Harvard Law School, Berkman Center for Internet & Society, 2007.

Gorman, Siobhan. "U.S. Official Warns About 'Anonymous' Power Play." *Wall Street Journal*, February 21, 2012. http://online.wsj.com/news/articles/SB10001424052970204059804577229390105521090.

The Guardian. "FBI Warns That Anonymous Has Hacked US Government Sites for a Year." November 16, 2013. http://www.theguardian.com/technology/2013/nov/16/anonymous-fbi.

Hall, Camilla and Javier Blas. "Aramco Cyber Attack Targeted Production." *Financial Times*, December 10, 2012. http://www.ft.com/cms/s/0/5f313ab6-42da-11e2-a4e4-00144feabdc0.html#axzz3Af5d25Vk.

Halupka, Max. "The Evolution of Anonymous as a Political Actor." Master's thesis, Flinders University of South Australia, 2011.

Hands, Joss. *@ Is for Activism*. London, United Kingdom: Pluto Press, 2011.

Harding, Luke. "How Edward Snowden Went from Loyal NSA Contractor to Whistleblower." *The Guardian*, January 31, 2014. http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract.

Harris, Shane. "Black Market for Malware and Cyber Weapons Is Thriving." *Foreign Policy*. March 25, 2014. http://complex.foreignpolicy.com/posts/2014/03/24/black_market_for_malware_and_cyber_weapons_is_thriving.

Heath, Louis G. *Vandals in the Bomb Factory*. Metuchen, NJ: The Scarecrow Press, 1976.

Heimbach, Wayne and Bill Roberts. "A Look Back at the 1968 Democratic Convention." *International Socialist Review*, August 2008. http://www.isreview.org/issues/60/feat-chicago68.shtml.

Heineman, David Scott. "The Digital Rhetorics of Hacktivism: Anti-Institutional Politics in Cyberspace." Master's thesis, University of Iowa, 2007.

Hepworth, Daniel P. "Analysis of Al-Qaeda Terrorist Attacks to Investigate Rational Action." *Perspectives on Terrorism* 8, no. 3 (2014): 23–38. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/253/html.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49–60.

Ingalsbee, Timothy. "Earth First! Activism: Ecological Postmodern Praxis in Radical Environmentalist Identities." *Sociological Perspectives* 39, no. 2 (1996): 263–276.

Ingersoll, Geoffrey. "Here's Why the U.S. is Incredibly Vulnerable to Cyber Attacks." *Business Insider*, October 15, 2012. http://www.businessinsider.com/heres-why-the-us-is-incredibly-vulnerable-to-cyber-attacks-2012-10.

Isikoff, Michael. "Exclusive: Snowden Swiped Password from NSA Coworker." *NBC News*, February 12, 2014. http://www.nbcnews.com/news/investigations/exclusive-snowden-swiped-password-nsa-coworker-n29006.

Iverson, David R. *The Ring of Gyges: Anonymity and Technological Advance's Effect on the Deterrence of Non-State Actors in 2035*. Montgomery, AL: Air War College, 2011. http://www.au.af.mil/au/awc/awcgate/awc/2011_iverson.pdf.

Jacobs, Ron. *The Way the Wind Blew: A History of the Weather Underground*. London, United Kingdom: Verso Books, 1997.

Jamison, Andrew. "Social Movements and Science: Cultural Appropriations of Cognitive Praxis." *Science as Culture* 15, no. 1 (March 2006): 45–59.

Jayakumar, Amrita. "Data Breach Hits Target's Profits, but That's Only the Tip of the Iceberg." *The Washington Post*, February 26, 2014. http://www.washingtonpost.com/business/economy/data-breach-hits-targets-profits-but-thats-only-the-tip-of-the-iceberg/2014/02/26/159f6846-9d60-11e3-9ba6-800d1192d08b_story.html.

Jenkins, Brian Michael. "The New Age of Terrorism." In *The McGraw-Hill Homeland Security Handbook*, edited by David Kamien, 117–130. New York: Mc-Graw Hill Companies, 2006. http://www.prgs.edu/content/dam/rand/pubs/reprints/2006/RAND_RP1215.pdf.

Johnston, Hank. *States and Social Movements*. Cambridge, United Kingdom: Polity Press, 2011.

Jordan, Tim and Paul Taylor. *Hacktivism and Cyberwars: Rebels with a Cause?* New York, New York; Taylor & Francis, 2004.

Joosse, Paul. "Leaderless Resistance and Ideological Inclusion: The Case of the Earth Liberation Front." *Terrorism and Political Violence* 19 (2007): 351–68.

Joseph, Kendall R. *Global Information Systems Threats: Issues in System Security in the New Age of Hactivism, Cyberterrorism and Cyberwarfare*. Murfreesboro, TN: Middle Tennessee State University, 2003. http://www.zachevans.org/wp-content/uploads/2012/02/Global_Information_Systems_Threats.pdf.

Karatnycky, Adrain. "Ukraine's Orange Revolution." *Foreign Affairs*, April 2005. http://www.foreignaffairs.com/articles/60620/adrian-karatnycky/ukraines-orange-revolution.

Kerr, Paul K. John Rollins, and Catherine Theohary. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. Washington, DC: Congressional Research Service, 2010. https://cyberwar.nl/d/R41524.pdf.

Kizza, Joseph Migga. *Computer Network Security and Cyber Ethics*. 2nd ed. Jefferson, NC: McFarland & Company, 2006.

Knefel, John. "Cyber-Activist Jeremy Hammond Sentenced to 10 Years in Prison." *Rolling Stone*, November 15, 2013. http://www.rollingstone.com/politics/news/cyber-activist-jeremy-hammond-sentenced-to-10-years-in-prison-20131115.

Landers, Chris. "Serious Business: Anonymous Takes on Scientology (and Isn't Afraid of Anything)." *Citypaper*, April 2, 2008. http://www2.citypaper.com/arts/story.asp?id=15543.

Liddick, Donald R. *Eco-Terrorism: Radical Environmental and Animal Liberation Movements*, Westport, CT: Praeger, 2006. http://sinzoofilikon.weebly.com/uploads/5/0/5/7/5057569/animal_terrorism.pdf.

Loadenthal, Michael. "The Earth Liberation Front: A Movement Analysis." *Radical Criminology*, no. 2 (2013): 15–46.

Luman, Stuart. "The Hacktivist." *Chicago*, June 25, 2007. http://www.chicagomag.com/Chicago-Magazine/July-2007/The-Hacktivist/.

Mauss, Armand L. “The Genesis of Social Problem-Movements.” In *Social Problems as Social Movements*, edited by Armand L. Mauss, 38–71. Philadelphia: J.B. Lippincott, Co., 1975. http://media.pfeiffer.edu/lridener/courses/spassm.html.

McCormick, Gordon H. “Terrorist Decision Making.” *Annual Review of Political Science* 6 (2003): 473–507.

McFadden, Robert. “Remembering Columbia, 1968.” *New York Times*, April 25, 2008. http://cityroom.blogs.nytimes.com/2008/04/25/remembering-columbia-1968/.

McLaughlin, Victoria. *Anonymous: What Do We Have to Fear from Hacktivism, the Lulz, and the Hive Mind?* Charlottesville, VA: University of Virginia, 2012. https://pages.shanti.virginia.edu/Victoria_McLaughlin/files/2012/04/McLaughlin_PST_Thesis_2012.pdf.

Midgley, Scott. *Peaceful Protest to Violent Revolution: The Evolution of SDS and the Weathermen*. Charles Town, WV: American Public University, 2011. http://www.academia.edu/1111206/Peaceful_Protest_to_Violent_Revolution_The_Evolution_of_SDS_and_the_Weathermen.

Miklaszewski, Jim and Courtney Kube. “Panetta: Cyber Intruders Have Already Infiltrated U.S. Systems.” *U.S. News*, October 11, 2012. http://usnews.nbcnews.com/_news/2012/10/11/14376572-panetta-cyber-intruders-have-already-infiltrated-us-systems?lite\.

Magnuson, Stew. “Growing Black Market for Cyber-Attack Tools Scares Senior DOD Official.” *National Defense Magazine*. February 22, 2013. http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1064.

Nakashima, Ellen and Marimow, Ann E. “Judge: NSA’s Collecting of Phone Records Is Probably Unconstitutional.” *The Washington Post*, December 16, 2013. http://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html.

National Council on Economic Education. *Thinking Globally: Effective Lessons for Teaching about the Interdependent World Economy: Lesson 1: Ten Basic Questions about Globalisation*. New York: National Council on Economic Education, 2005. http://www.imf.org/external/np/exr/center/students/hs/think/lesson1.pdf.

Norton, Quinn. “2011: The Year Anonymous Took on Cops, Dictators and Existential Dread.” *Wired*, January 11, 2012. http://www.wired.com/threatlevel/2012/01/anonymous-dicators-existential-dread/3/.

———. “Anonymous 101: Introduction to the Lulz.” *Wired*, November 8, 2011. http://www.wired.com/2011/11/anonymous-101/all/1.

———. “How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down.” *Wired*, July 3, 2012. http://www.wired.com/2012/07/ff_anonymous/all/.

NPR. “Transcript of President Obama’s Speech on NSA Reforms.” January 17, 2014. http://www.npr.org/blogs/itsallpolitics/2014/01/17/263480199/transcript-of-president-obamas-speech-on-nsa-reforms.

Olson, Dean T. “The Path to Terrorist Violence: A Threat Assessment Model for Radical Groups at Risk of Escalation to Acts of Terrorism.” Master’s thesis, Naval Postgraduate School, 2005.

Olson, Parmy. “FBI Agent’s Laptop ‘Hacked’ To Grab 12 Million Apple IDs—UPDATED.” *Forbes*, September 4, 2012. http://www.forbes.com/sites/parmyolson/2012/09/04/fbi-agents-laptop-hacked-to-grab-12-million-apple-ids-anonymous-claims/.

———. *We Are Anonymous*. New York: Little, Brown and Company, 2012.

Paget, Francois. *Cybercrime and Hacktivism*. McAfee Labs. http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf.

Patrikakis, Charalampos, Michalis Masikos, and Olga Zouraraki. “Distributed Denial of Service Attacks.” *The Internet Protocol Journal* 7, no. 4 (2004): 13–35. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/ipj_7-4.pdf.

Perlroth, Nicole. “Cyberattack on Saudi Oil Firm Disquiets U.S.” *New York Times*, October 23, 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0.

Philippon, Daniel J. “Edward Abbey’s Remarks at the Cracking of Glen Canyon Dam.” *Oxford Journals: ISLE* 11, no. 2 (2004): 161–66.

Porche III, Issac R., Jerry M. Sollinger, and Shawn McKay. *A Cyberworm That Knows No Boundaries*. Occasional paper. Santa Monica, CA: RAND Corporation, 2011. http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf.

Puzzanghera, Jim. “Scientology Feud with Its Critics Takes to Internet.” *LA Times*, February 5, 2005. http://www.latimes.com/local/la-me-scientology5feb05-story.html.

Reitman, Janet. “Jeremy Hammond: Rise and Fall of the Legendary Hacker.” *Rolling Stone*, December 7, 2012. http://www.rollingstone.com/culture/news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-20121207?print=true.

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013.

Richards, Jason. “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security.” *International Affairs Review*. Accessed March 29, 2014. http://www.iar-gwu.org/node/65.

Rishikof, Harvey and Bernard Horowitz. *Shattered Boundaries: Whither the Cyber Future*. Calgary, Alberta, Canada: Centre of Military and Strategic Studies, 2012.

Samuel, Alexandra. “Hacktivism and the Future of Political Participation.” Master’s thesis, Harvard University, 2004. http://www.academia.edu/616169/Hacktivism_and_the_future_of_political_participation.

———. *Decoding Hacktivism: Purpose, Method, and Identity in a New Social Movement*. Cambridge, MA: Harvard University, 2001. http://www.alexandrasamuel.com/netpolitics/decodinghacktivism.pdf.

Sanger, David E. “Obama Ordered Wave of Cyberattacks against Iran.” *New York Times*, June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2&partner=rss&emc=rss&.

Schachtman, Noah. “Kremlin Kids: We Launched the Estonian Cyber War.” *Wired*, March 11, 2009. http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/.

Schleimer, Lauren. “Schleimer ‘12: What Happened to Student Activism?” *Brown Daily Herald*, March 8, 2012. http://www.browndailyherald.com/2012/03/08/schleimer-12-what-happened-to-student-activism/.

Schwartz, Seth, Curtis Dunkel, and Alan Waterman. *Terrorism: An Identity Theory Perspective, Studies in Conflict & Terrorism*. New York: Routledge, 2008.

Snow, David A. and Robert D. Benford. “Ideology, Frame Resonance, and Participant Mobilization.” In *From Structure to Action: Social Movement Participation across Cultures*, edited by Bert Klandermans, Hanspeter Kriesi, and Sidney Tarrow, 197–217. Greenwich, CT: JAI Press, 1988.

Sterner, Eric. *The Paradox of Cyber Protest*. Arlington, VA: George C. Marshall Institute, 2012. http://marshall.org/wp-content/uploads/2013/12/Paradox-PO-Apr-12.pdf.

Stuart, Keith. “Why Are Lulzsec and Anonymous Hacking Games Companies?” *The Guardian*, June 16, 2011. http://www.theguardian.com/technology/2011/jun/16/lulzsec-anonymous-hacking-games-companies.

Symantec. *Advanced Persistent Threats: A Symantec Perspective*. Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

Taft, Philip and Philip Ross. “American Labor Violence: Its Causes, Character, and Outcome.” In *The History of Violence in America: A Report to the National Commission on the Causes and Prevention of Violence*, edited by Hugh Davis Graham and Ted Robert Gurr, 1969. http://www.ditext.com/taft/violence.html.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardians*, May 16, 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

Tropina, Tatiana. “Cyber Crime and Organized Crime.” *F3 Magazine*. Accessed August 3, 2014. http://f3magazine.unicri.it/?p=310z.

Tusa, Felix. “How Social Media Can Shape a Protest Movement: The Cases of Egypt in 2011 and Iran in 2009.” *Arab, Media & Society*, no. 17 (2013). http://www.arabmediasociety.com/?article=816.

U.S. Government Accountability Office. *Protecting the Federal Government’s Information Systems and Nation’s Cyber Critical Infrastructures*. 2013. http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study.

Varon, Jeremy. *Bringing the War Home*. Berkley, CA: University of California Press, 2004.

Verizon. *2012 Data Breach Investigations Report*. Verizon Enterprise. 2012. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

———. *2013 Data Breach Investigations Report*, Verizon Enterprise. 2013. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

Wallace, Gregory. “Target and Neiman Marcus Hacks: The Latest.” *CNN Money*. January 13, 2014. http://money.cnn.com/2014/01/13/news/target-neiman-marcus-hack/.

Wallace, Patricia. *The Psychology of the Internet*. Cambridge, United Kingdom: Cambridge University Press, 2001.

Waterman, Shaun. “Cold War Throwback: U.S.-Russia to Use Nuclear ‘Hotline’ for New Cyber Showdown.” *The Washington Times*, June 18, 2013. http://www.washingtontimes.com/news/2013/jun/18/cold-war-throwback-us-russia-use-nuclear-hotline-n/.

Watts, Susan. “Newsnight Online ‘Chat’ with Lulz Security Hacking Group.” *BBC News*, June 24, 2011. http://www.bbc.co.uk/news/technology-13912836.

Weaponized Malware: A Clear and Present Danger (WP-EN-09-12-12). Lumension. September 2012. https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Whitepapers/Weaponized-Malware---A-Clear-and-Present-Danger.aspx.

Weinberger, Sharon. “Top Ten Most-Destructive Computer Viruses.” *Smithsonian*. March 19, 2012. http://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/.

White House. *Strategy to Combat Transnational Organized Crime*. Washington, DC: Executive Office of the President, 2011. http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

Wilshusen, Gregory C. *Cybersecurity: Threats Impacting the Nation*. Washington, DC: U.S. Government Accountability Office, 2012. http://www.gao.gov/assets/600/590367.pdf

Winter, Jana. “16 Suspected ‘Anonymous’ Hackers Arrested in Nationwide Sweep.” *Fox News*, July 19, 2011. http://www.foxnews.com/tech/2011/07/19/exclusive-fbi-search-warrants-nationwide-hunt-anonymous/.

Wirtz, James J., Colin S. Gray, and John Baylis. *Strategy in the Contemporary World: An Introduction to Strategic Studies*. Kindle Edition. Oxford, United Kingdom: Oxford University Press, 2012.

Wright, Rebecca. “Hives, Damn Hives, and the Internet.” *The Morningside Review*, July 11, 2014. http://morningsidereview.org/essay/hives-damn-hives-and-the-Internet/.

World Economic Forum. *Global Risks 2014*. 9th ed. Geneva, Switzerland: World Economic Forum, 2014. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf.

Worthen, Ben, Russel Adams, Nathan Hodge, and Evan Ramstad. “Lockheed, PBS Join Roster of Hacking Victims.” *The Wall Street Journal*, May 31, 2011. http://online.wsj.com/news/articles/SB10001424052702304563104576355623894502788.

Yalamarthy, Neelkiran. “Profs See Waning Student Activism.” *Brown Daily Herald*, October 25, 2011. http://www.browndailyherald.com/2011/10/25/profs-see-waning-student-activism/.

Yin, Sara. “‘Anonymous’ Attacks Sony in Support of PS3 Hackers.” *PCMag*. April 4, 2011. http://www.pcmag.com/article2/0,2817,2383018,00.asp.

Zimbardo, Philip. *The Lucifer Effect: Understanding How Good People Turn Evil*. New York: Random House Trade Paperbacks, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California